现代数学基础丛书 102

矩阵结合方案

王仰贤 霍元极 麻常利 著



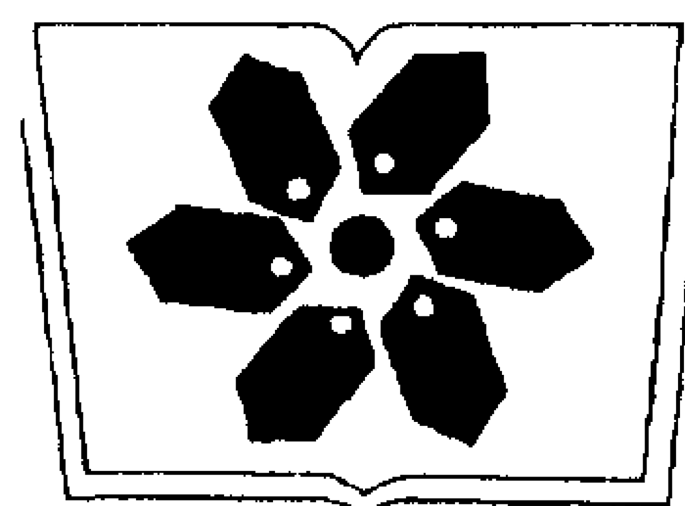
科学出版社
www.sciencep.com

(O-2592.0101)



销售分类建议：高等数学

ISBN 7-03-018032-1
定 价：45.00 元



中国科学院科学出版基金资助出版

现代数学基础丛书　102

矩阵结合方案

王仰贤　霍元极　麻常利　著

科 学 出 版 社
北　京

内 容 简 介

本书论述有限域上各类典型矩阵在群作用下构作的结合方案,其内容主要包括有限域上的长方矩阵、交错矩阵、Hermite矩阵、对称矩阵和二次型构作的结合方案,导出各类结合方案的一般参数计算公式,讨论这些结合方案的本原性、对偶性、P 多项式等基本性质以及自同构群. 特别论述了特征数为 2 时二次型结合方案的特征值及其聚合方案的对偶方案.

本书可供大专院校数学与信息专业高年级学生、研究生、教师及有关数学工作者阅读,也可供其他有关科技工作者参考.

图书在版编目(CIP)数据

矩阵结合方案/王仰贤, 霍元极, 麻常利著. 一北京: 科学出版社, 2006

(现代数学基础丛书;102/杨乐主编)

ISBN 7-03-018032-1

I.矩… II.①王… ②霍… ③麻… III.矩阵-结合方案 IV. O151.21

中国版本图书馆CIP数据核字(2006) 第107552号

责任编辑: 吕 虹 / 责任校对: 刘亚琦

责任印制: 安春生 / 封面设计: 王 浩

科学出版社 出版

北京东黄城根北街16号

邮政编码: 100717

http://www.sciencep.com

源海印刷有限责任公司 印刷

科学出版社发行 各地新华书店经销

*

2006年9月第 一 版 开本: B5(720×1000)

2006年9月第一次印刷 印张: 18

印数: 1—3 000 字数: 328 000

定价: 45.00 元

(如有印装质量问题, 我社负责调换〈路通〉)

《现代数学基础丛书》序

对于数学研究与培养青年数学人才而言，书籍与期刊起着特殊重要的作用．许多成就卓越的数学家在青年时代都曾钻研或参考过一些优秀书籍，从中汲取营养，获得教益．

20 世纪 70 年代后期，我国的数学研究与数学书刊的出版由于文化大革命的浩劫已经破坏与中断了十余年，而在这期间国际上数学研究却在迅猛地发展着．1978 年以后，我国青年学子重新获得了学习、钻研与深造的机会．当时他们的参考书籍大多还是 50 年代甚至更早期的著述．据此，科学出版社陆续推出了多套数学丛书，其中《纯粹数学与应用数学专著》丛书与《现代数学基础丛书》更为突出，前者出版约 40 卷，后者则逾 80 卷．它们质量甚高，影响颇大，对我国数学研究、交流与人才培养发挥了显著效用．

《现代数学基础丛书》的宗旨是面向大学数学专业的高年级学生、研究生以及青年学者，针对一些重要的数学领域与研究方向，作较系统的介绍．既注意该领域的基础知识，又反映其新发展，力求深入浅出，简明扼要，注重创新．

近年来，数学在各门科学、高新技术、经济、管理等方面取得了更加广泛与深入的应用，还形成了一些交叉学科．我们希望这套丛书的内容由基础数学拓展到应用数学、计算数学以及数学交叉学科的各个领域．

这套丛书得到了许多数学家长期的大力支持，编辑人员也为其付出了艰辛的劳动．它获得了广大读者的喜爱．我们诚挚地希望大家更加关心与支持它的发展，使它越办越好，为我国数学研究与教育水平的进一步提高作出贡献．

杨　乐

2003 年 8 月

序　言

结合方案原是伴随于部分平衡不完全区组设计的一个组合结构, 描述具有多个结合关系的处理之间的某种平衡性,1952 年由 R.C. Bose 和 T.Shimamoto 引进. 由于它和编码、图论及有限群的密切联系, 特别是给编码提供了某种理论框架, 到 20 世纪 80 年代, 结合方案的研究已发展成为代数组合学中的一个重要分支. 它吸引了越来越多的人进行研究, 所涉及的内容逐步扩大, 研究方法各有所长.

我国结合方案的研究始于 20 世纪 50 年代末. 开始有许宝騄、张里千教授的著名成果, 随后, 我和当时的几位学生以典型群作用下各种类型的子空间作处理和区组来构作结合方案和设计并计算了它们的参数, 所得成果汇集于《有限几何与不完全区组设计的一些研究》(万哲先, 戴宗铎, 冯绪宁, 阳本傅著.1966. 北京：科学出版社) 这部专著里. 在 20 世纪 60 年代中, 我又取 n 阶 Hermite 矩阵构作了一类结合方案, 并计算了低阶情形的参数 (《中国科学》, 1965), 开创了利用矩阵构作结合方案的新方向. 后来发展起来的结合方案研究说明, 那时利用极大全迷向子空间构作的结合方案和利用 Hermite 矩阵构作的结合方案均为所谓的本原 P 多项式和 Q 多项式结合方案的基本类型.

20 世纪 70 年代末, 王仰贤教授继续了利用矩阵构作结合方案这项研究, 他除了对于 Hermite 矩阵结合方案的参数给出了计算公式以外, 还研究了长方矩阵结合方案和交错矩阵结合方案. 随后霍元极、祝学理教授和我研究了特征数不为 2 的域上对称矩阵结合方案. 到了 20 世纪 90 年代, 王仰贤教授又和他的学生马建敏、麻常利博士研究特征数为 2 的有限域上更为复杂的对称矩阵结合方案和二次型结合方案. 他们除讨论这两类结合方案的参数计算外, 还讨论了它们的结合子方案及相应的商方案, 这两类结合方案的对偶性, 以及二次型结合方案的自同构和特征值等等. 这样矩阵结合方案的研究日趋完整. 现在王仰贤、霍元极教授和麻常利博士把矩阵结合方案方面的成果进行综合、扩充和系统化, 汇编成书, 其目的是系统阐述各类矩阵结合方案的构作, 参数计算以及它们的结构, 包括本原性、对偶性、P(和 Q) 多项式性质以及自同构等. 我相信这本专著的出版会为学习和研究结合方案的读者提供一些研究方法和工具. 更希望读者在结合方案的研究上, 取得一些新的成果.

万哲先

2006 年 3 月

前　言

本书是遵照万哲先院士的建议，把我们 (和合作者) 关于矩阵结合方案研究的成果进行了综合、扩充和系统化而形成的.

全书共八章. 第一章介绍结合方案的一般基础性理论，主要包括结合方案的基本性质、Krein 参数、对偶性、本原性、结合子方案和商方案等概念，为初学者阅读后面的章节提供了比较系统而又必需的预备知识. 这些内容主要取自参考文献 [2]. 从第二章到第七章，分别阐述有限域上各类矩阵结合方案，即由长方矩阵、交错矩阵、Hermite 矩阵、对称矩阵和二次型构成的结合方案，讨论它们的构作、参数计算和结构 —— 对偶性、本原性、P 多项式以及自同构等. 最后在第八章中讨论特征数为 2 的二次型结合方案的特征值及其聚合方案的对偶方案.

这些矩阵结合方案被统一地看作某矩阵类 (作成加法群) 上的合同变换和平移生成的群作用下自然地导出来的. 由于它们的构作依赖于矩阵类在一般线性群作用下的合同标准型，所以在讨论它们的参数计算时，借助文献 [15] 中给出的典型几何中各种类型子空间的计数公式就是一种有效的办法. 为了内容的完整和使初学者熟练矩阵方法，对于几类距离正则图的参数，本书中也给出了矩阵方法的再证明. 关于书中各类矩阵结合方案的自同构之确定，归结到文献 [16] 中著名的各类矩阵几何基本定理. 对于特征数为 2 的 n 元二次型采用了文献 [15] 中的矩阵形式，相应结合方案的自同构之确定，在 $n \geqslant 3$ 时是借助了文献 [12] 中二次型图的自同构之结果，而对于 $n = 2$ 的情形则是巧妙地应用纯矩阵方法得到的. 因此，本书所阐述的矩阵结合方案，就其历史背景和讨论的内容以及所用的方法而言，实为由华罗庚、万哲先创导的具有独特风格的"矩阵方法"在结合方案研究方面的应用与发展.

本书的第二章到第七章基本上是彼此独立的，读者在阅读了第一章之后可以根据兴趣选读后面的章节，在掌握了一定的方法与技巧后即可进行一些课题研讨. 当然，如前所述，读者需要了解文献 [15] 和 [16] 中的有关内容. 此外，各章还涉及到有限群的特征标知识，读者可从一般群论书籍中找到，也可参阅文献 [2].

本书中有不少内容是没有发表过的，不妥之处，敬请读者指正.

万哲先院士对本书的撰写和出版给予了热情的指导和支持，并为本书作序，我们表示衷心的感谢. 冯荣权教授和马建敏博士整理了本书第八章部分内容的初稿，高锁刚教授用本书初稿的部分内容作为他的研究生学习结合方案时的教材，王恺顺教授在本书付印前仔细阅读了全稿，并进行了核算，他们都提出了宝贵意见. 河北师范大学对本书的撰写和出版在经费等多方面给予了很大支持；中国科学院科学出

版基金委员会为本书出版给予了资助; 科学出版社吕虹编审对本书出版给予了大力的帮助. 在此, 我们一并表示诚挚感谢.

王仰贤　霍元极　麻常利
2006 年 4 月

符 号 表

符号	含义
$\|X\|$	集合X中元素个数
R_i	结合类或结合关系
$\mathfrak{X} = (X, \{R_i\}_{0\leqslant i\leqslant d})$	类数为d的结合方案
k_i	R_i的价
p_{ij}^k	$\mathfrak{X}$的交叉数
A_i	结合关系R_i的邻接矩阵
$\mathfrak{A}$	$\mathfrak{X}$的邻接代数
$M_n(\mathbb{C})$	复数域$\mathbb{C}$上的n阶全阵代数
$\mathcal{B}$	$\mathfrak{X}$的交叉代数
Ω	有限集合
G	有限群
Λ_i	G作用在$\Omega\times\Omega$上的轨道
$\mathbb{A}(\sigma)$	阶为$\|G\|$的矩阵, 其中(x, y)位置的元素是$\delta_{x^\sigma y}$
$\mathbb{X}_i$	$\sum_{x\in X_i} x$, 有限群X的子集X_i中元素的形式和
U	n阶酉矩阵
V	$\mathbb{C}$上的n维向量空间
E_i	$V = V_0\perp V_1\perp\cdots\perp V_r$到$V_i$的正射影在标准正交基$\{e_x\|x\in X\}$下的矩阵
$p_i(j)$	A_i在V_j上的特征值
m_i	$\mathfrak{X}$的重数
$q_i(j)$	满足$E_i = \frac{1}{\|X\|}\sum_{j=0}^d q_i(j)A_j$ $(i = 0, 1, \cdots, d)$的数
$P = (p_i(j))$	第一特征值矩阵, 其中(j, i)元素为$p_i(j)$
$Q = (q_i(j))$	第二特征值矩阵, 其中(j, i)元素为$q_i(j)$
$\circ$	Hadamard乘积符号
C_i	有限群G的共轭类
χ_i	群G的特征标
$\mathbb{C}_i$	$\sum_{x\in C_i} x$

$\widehat{\mathfrak{A}}$	$\mathfrak{A}$的对偶代数
q_{ij}^k	Krein参数
$\widehat{B}_i$	$(j,\ k)$位置的元素为q_{ij}^k的$d+1$阶矩阵
$\mathbb{C}[X]$	有限群 X 在复数域 $\mathbb{C}$ 上的群环 (代数)
$\mathfrak{S}$	由$\mathbb{X}_0, \mathbb{X}_1, \cdots, \mathbb{X}_d$生成的$S$一环
$\mathfrak{X}(\mathfrak{S})$	$\mathfrak{S}$的结合方案
$\Delta_i,\ \Delta_i^*$	$\mathbb{C}(X)$到$\mathbb{C}$的线性映射
$\mathbb{Y}_i$	$\sum_{\alpha\in s_i}\Delta_\alpha^*$, 其中$s_0, s_1, \cdots, s_d$是$\{0,1,\cdots,$ $n-1\}$的一个分划
$\mathfrak{S}^*$	$\langle\mathbb{Y}_0, \mathbb{Y}_1, \cdots, \mathbb{Y}_d\rangle$, $\mathfrak{S}$的对偶S环
$\Gamma^{(i)}$	关系R_i的图, 即以X为顶点集而以R_i为边集的图
G_x	有限群作用在有限集Ω上, $x\in\Omega$的稳定子
$\bigotimes$	Kronecker积
$\mathfrak{X}(\Sigma)$	结合方案 $\mathfrak{X}$ 在非本原系 Σ 上导出的商结合方案
∂	图的距离函数
$\Gamma_i(x)$	在图Γ中与顶点x距离为i的顶点的集合
$\Gamma(x)$	$\Gamma_1(x)$
c_i	$\lvert\Gamma_{i-1}(x)\cap\Gamma(y)\rvert$, 其中$y$, x是Γ的两个顶点, $\partial(y,x)=i$.
a_i	$\lvert\Gamma_i(A)\cap\Gamma(B)\rvert$
b_i	$\lvert\Gamma_{i+1}(A)\cap\Gamma(B)\rvert$
$\mathrm{Aut}(\Gamma)$	图 Γ 的自同构群
$\mathrm{Aut}(\mathfrak{X})$	结合方案 $\mathfrak{X}$ 的自同构群
Inn	内自同构
$\mathbb{F}_q$	q个元素的有限域
$n_i(m\times n,\ q)$	M_{mn}中秩为 i 的 $m\times n$矩阵的个数
$\mathrm{Mat}(m\times n,\ q)$	长方矩阵结合方案
$GL_n(\mathbb{F}_q)$	$\mathbb{F}_q$上的n级线性群
ϕ_A	映射符号, 其中$A=(a_{ij})$,
$\mathcal{K}(n,\ q)$	$\mathbb{F}_q$上全体$n\times n$交错矩阵的集合
$\mathrm{Alt}(n,\ q)$	$\mathbb{F}_q$上n阶交错矩阵结合方案
$Sp_{2\nu}(K_\nu, \mathbb{F}_q)$	$\mathbb{F}_q$上关于$K_\nu=\begin{pmatrix} 0 & I^{(\nu)} \\ -I^{(\nu)} & 0 \end{pmatrix}$的$2\nu$阶辛群

$N(m,\ s;\ 2\nu)$	辛空间 $\mathbb{F}_q^{(2\nu)}$ 中 $(m,\ s)$ 型子空间的个数
$K_i(n,\ q)$	$\mathbb{F}_q$ 上秩为 $2i$ 的 $n\times n$ 交错矩阵的个数
$\mathbb{F}_q^*$	$\mathbb{F}_q$ 的乘法群
$\mathcal{H}(n,\ q^2)$	$\mathbb{F}_{q^2}$ 上全体 Hermite 矩阵的集合
$\mathrm{Her}(n,\ q^2)$	$\mathbb{F}_{q^2}$ 上 n 阶 Hermite 矩阵结合方案
$U_n(H,\ \mathbb{F}_{q^2})$	$\mathbb{F}_{q^2}$ 上关于 H 的 n 级 U 群
$N(m,\ r;\ n)$	酉空间 $\mathbb{F}_{q^2}^{(n)}$ 中 $(m,\ r)$ 型子空间的个数
$H_i(n,\ q^2)$	$\mathbb{F}_{q^2}$ 上秩为 i 的 $n\times n$ Hermiti 矩阵的个数
$S(n,\ q)$	$\mathbb{F}_q$ 上全体 $n\times n$ 对称矩阵的集合
$\mathrm{Sym}(n,\ q)$	$\mathbb{F}_q$ 上 n 阶对称矩阵结合方案
$C_{(i,\xi)}$	$\{X\in S(n,q) \mid X\sim[I^{(i-1)},\xi,0^{(n-i)}],0\leqslant i\leqslant n,$ $\xi=1$ 或 $z\}$
$R_{(i,\xi)}$	对应于 $C_{(i,\ \xi)}$ 的结合类
$k_{(i,\ \xi)}, k_{(i,\ \xi)}(n)$	$R_{(i,\ \xi)}$ 的价
$p_{(i,\eta)(j,\zeta)}^{(k,\xi)}, p_{(i,\eta)(j,\zeta)}^{(k,\xi)}(n)$	$\mathrm{Sym}(n,q)$ 的交叉数
$\Gamma^{(i,\xi)}$	$R_{(i,\xi)}$ 的关系图, $\xi=1$ 或 z
$S_{2\nu+\delta,\Delta}$	$\mathbb{F}_q$ 上的对称矩阵 $\left[\begin{pmatrix} 0 & I^{(\nu)} \\ I^{(\nu)} & 0 \end{pmatrix}, \Delta\right]$
$O_{2\nu+\delta,\Delta}(\mathbb{F}_q)$	奇特征的 $\mathbb{F}_q$ 上关于 $S_{2\nu+\delta,\Delta}$ 的 $2\nu+\delta$ 级正交群
$N(m,2s+\gamma,s,\Gamma;2\nu+\delta,\Delta)$	正交空间 $\mathbb{F}_q^{(2\nu+\delta)}$ 中 $(m,2s+\gamma,s,\Gamma)$ 型子空间的个数
$\overline{R}_i$	$\{(X,Y) \mid X,Y\in S(n,q),\ \mathrm{rank}(X-Y)=2i-1$ 或 $2i\}(0\leqslant i\leqslant[\frac{n+1}{2}])$
$\mathrm{Quad}(n,q)$	结合方案 $(S(n,q),\{\bar{R}_i\}_{0\leqslant i\leqslant[\frac{n+1}{2}]})$
$Ps_{2\nu+\delta}(\mathbb{F}_q)$	偶特征的 $\mathbb{F}_q$ 上关于 $S_{2\nu+\delta,\Delta}$ 的伪辛群
$N(m,2s+\tau,s,\varepsilon;2\nu+\delta)$	伪辛空间 $\mathbb{F}_q^{(2\nu+\delta)}$ 中 $(m,2s+\tau,s,\varepsilon)$ 型子空间的个数
$t(S)$	偶特征的 $\mathbb{F}_q$ 上对称矩阵 S 的类型
$\overline{\mathrm{Sym}}(n,\ q)$(特征为 2)	以 $\overline{R}_i$ 为结合类的 P 多项式结合方案
$\equiv$	同余号
B_f	相伴于二次型 f 的对称双线性型
$Q(n,q)$	偶特征的 $\mathbb{F}_q$ 上全体 n 元二次型的集合
$\mathrm{Qua}(n,q)$	偶特征的 $\mathbb{F}_q$ 上二次型结合方案
Tr	$\mathbb{F}_q$ 在 $\mathbb{F}_2$ 上的迹

$O_n(\mathbb{F}_q, G)$	偶特征的$\mathbb{F}_q$上关于G的n级正交群, 其中G是$n\times n$正则矩阵
$N(m, 2s+\gamma, s, \Gamma; 2\nu+\delta)$	正交空间$\mathbb{F}_q^{(2\nu+\delta)}$中$(m, 2s+\gamma, s, \Gamma)$型子空间的个数
$Q_i(n, q)$	$Q(n, q)$中类型为i的二次型集合
$k_{2s+\gamma}(n)$	$\mathrm{Qua}(n, q)$的结合类$R_{2s+\gamma}$的价
$p^{2j_1+\delta_1}_{2j_2+\delta_2,\, 2j_3+\delta_3}(n)$	Qua(n, q)的交叉数
$\widetilde{\mathrm{Q}}\mathrm{ua}(n, q)$	$\mathrm{Qua}(n, q)$的聚合方案
$C_k^{(n)}$	$\mathbb{F}_q$上型为k的n元二次型的“合同类”, $k\in\{0, 1, 2^+, 2^-, 3, \cdots\}$
$f_i^{(n)}$	偶特征的$\mathbb{F}_q$上$S(n, q)$的合同类D_i中矩阵给出的特征标
$f_r^{(m)}$	偶特征的$\mathbb{F}_q$上$S(n, q)$中秩为r的非交错矩阵给出的特征标
$f_{2k^*}^{(n)}$	偶特征的$\mathbb{F}_q$上秩为$2k$的交错矩阵给出的特征标
$\widetilde{\mathrm{S}}\mathrm{ym}\,(n, q)$	偶特征的$\mathbb{F}_q$上$\mathrm{Sym}(n, q)$的一个聚合方案

目　录

*　　*　　*

第一章　结合方案理论基础

§1.1　结合方案的基本概念

设 X 是一个非空有限集合, $|X| = n$. $R_0, R_1, \cdots, R_d$ 是 $X \times X$ 的非空子集且满足下面的条件:

(i) $R_0 = \{(x, x)|x \in X\}$;

(ii) $X \times X = R_0 \cup R_1 \cup \cdots \cup R_d$, 且对所有 $i \neq j$, $R_i \cap R_j = \varnothing$;

(iii) 令 ${}^tR_i = \{(x,y)|(y,x) \in R_i\}$. 对于每个 $i \in \{0, 1, \cdots, d\}$, 存在 $i' \in \{0, 1, \cdots, d\}$ 使得 ${}^tR_i = R_{i'}$.

(iv) 对于任意 $i, j, k \in \{0, 1, \cdots, d\}$ 及任意一个对子 $(x, y) \in R_k$, 数

$$p_{ij}^k = |\{z \in X|(x, z) \in R_i,\ (z, y) \in R_j\}|$$

与 i, j, k 有关, 而与 R_k 中 (x, y) 的选取无关. 这样的一个构形 $\mathfrak{X} = (X, \{R_i\}_{0 \leqslant i \leqslant d})$ 叫做 X 上的一个类数为 d 的结合方案, R_i 叫做 $\mathfrak{X}$ 的第 i 个结合类 (或结合关系). 这些非负整数 p_{ij}^k 叫做 $\mathfrak{X}$ 的交叉数. 如果结合方案 $\mathfrak{X}$ 还满足条件:

(v) $p_{ij}^k = p_{ji}^k$ 对所有 $i, j, k \in \{0, 1, \cdots, d\}$,

那么 $\mathfrak{X}$ 就叫做一个交换结合方案. 如果结合方案 $\mathfrak{X}$ 满足条件:

(vi) $i' = i$, 对每个 $i \in \{0, 1, \cdots, d\}$,

那么 $\mathfrak{X}$ 就叫做一个对称结合方案(或者 Bose-Mesner 型结合方案).

容易看出, 如果结合方案 $\mathfrak{X}$ 是对称的, 那么它必为交换的. 反之, 交换结合方案未必是对称的.

在下面的讨论中, 我们恒设 $\mathfrak{X}$ 是交换的, 除非另有说明.

对于交换结合方案 $\mathfrak{X} = (X, \{R_i\}_{0 \leqslant i \leqslant d})$, 我们令 $k_i = p_{ii'}^0$ $(i = 0, 1, \cdots, d)$, 就是说, 对于任意取定的一个元素 $x \in X$, 存在 k_i 个元素 $y \in X$ 使得 $(x, y) \in R_i$. 数 k_i 叫做 R_i 的价(valency). 显然有

$$k_0 = 1,\ k_i = k_{i'},\ |X| = k_0 + k_1 + \cdots + k_d.$$

命题 1.1　对于交换结合方案 $\mathfrak{X}$ 的交叉数 p_{ij}^k, 我们有如下基本性质:

(i) $p_{0j}^k = \delta_{jk}$,

(ii) $p_{i0}^k = \delta_{ik}$,

(iii) $p_{ij}^0 = k_i \delta_{ij'}$,

(iv) $p_{ij}^k = p_{i'j'}^{k'}$,

(v) $\sum_{j=0}^d p_{ij}^k = k_i$,

(vi) $k_\gamma p_{\alpha\beta}^\gamma = k_\beta p_{\alpha'\gamma}^\beta = k_\alpha p_{\gamma\beta'}^\alpha$,

(vii) $\sum_{\alpha=0}^d p_{ij}^\alpha p_{k\alpha}^l = \sum_{\beta=0}^d p_{ki}^\beta p_{\beta j}^l$.

证明 (i) 取定 $(x, y) \in R_k$, 那么

$$p_{0j}^k = |\{z \in X|(x, z) \in R_0, (z, y) \in R_j\}|.$$

由 $(x, z) \in R_0$ 必有 $z = x$. 如果 $j \neq k$, 那么这样的 z 是不存在的; 如果 $j = k$, 这样的 z 只能是 x, 因此 (i) 成立.

(ii) 由交换性及 (i) 可得.

(iii) 任意取定一个元素 $x \in X$, 那么

$$p_{ij}^0 = |\{z \in X|(x, z) \in R_i, (z, x) \in R_j\}|.$$

如果 $j' \neq i$, 那么满足这样条件的 z 不存在; 如果 $j' = i$, 那么满足这样条件的 z 恰有 k_i 个. 因此 (iii) 成立.

(iv) 任意取定 $(x, y) \in R_k$, 那么 $(y, x) \in R_{k'}$, 并且

$$\begin{aligned} p_{ij}^k =& |\{z \in X|(x, z) \in R_i,\ (z, y) \in R_j\}| \\ =& |\{z \in X|(z, x) \in R_{i'},\ (y, z) \in R_{j'}\}| = p_{j'i'}^{k'}. \end{aligned}$$

由于 $\mathfrak{X}$ 是交换结合方案, 所以 $p_{j'i'}^{k'} = p_{i'j'}^{k'}$, 因此 (iv) 成立.

(v) 取定 $(x, y) \in R_k$, 那么有 k_i 个 z 使得 $(x, z) \in R_i$, 其中有 p_{ij}^k 个 z 满足 $(z, y) \in R_j$, 于是 $\sum_{j=0}^d p_{ij}^k = k_i$, 因此 (v) 成立.

(vi) 计算满足下面条件的三元组 (x, y, z) 的个数:

$$(x, y) \in R_\gamma,\ \ (x, z) \in R_\alpha,\ \ (z, y) \in R_\beta.$$

取定 x, 使 $(x, y) \in R_\gamma$ 的 y 有 k_γ 个. 对于每个这样的 y 有 $p_{\alpha\beta}^\gamma$ 个 z 使得 $(x, z) \in R_\alpha$ 及 $(z, y) \in R_\beta$. 因此满足上面条件的三元组 (x, y, z) 的个数为 $|X|k_\gamma p_{\alpha\beta}^\gamma$.

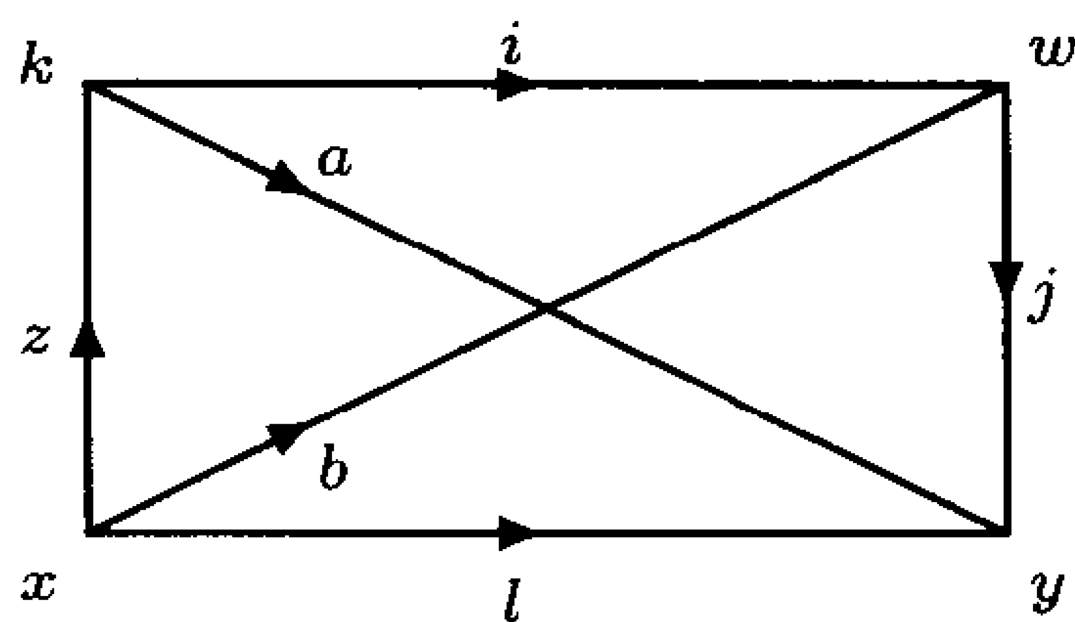
若先取 z, 那么满足 $(z, y) \in R_\beta$ 的 y 有 k_β 个. 对于每个这样的 y 有 $p_{\alpha'\gamma}^\beta$ 个 x 满足 $(x, z) \in R_\alpha$ 及 $(x, y) \in R_\gamma$. 因此满足上面条件的三元组 (x, y, z) 的个数为 $|X|k_\beta p_{\alpha'\gamma}^\beta$.

同理, 若先取定 x, 满足 $(x, z) \in R_\alpha$ 的 z 有 k_α 个. 对于每个这样的 z 有 $p_{\gamma\beta'}^\alpha$ 个 y 满足 $(x, y) \in R_\gamma$ 及 $(y, z) \in R_{\beta'}$. 因此满足上面条件的三元组 (x, y, z) 的个数为 $|X|k_\alpha p_{\gamma\beta'}^\alpha$. 这就证明了 (vi) 成立.

(vii) 对于一个取定的对子 $(x, y) \in R_l$, 计算满足下面条件的对子 (z, w) 的个数:

$$(x, z) \in R_k,\ \ (z, w) \in R_i,\ \ (w, y) \in R_j.$$

用下面的图表示这些关系：



对于 $\alpha \in \{0, 1, \cdots, d\}$, 满足条件 $(x, z) \in R_k$ 及 $(z, y) \in R_\alpha$ 的 z 有 $p^l_{k\alpha}$ 个, 对于每个这样的 z, 满足条件 $(z, w) \in R_i$ 及 $(w, y) \in R_j$ 的 w 有 p^α_{ij} 个. 因此, 满足条件的 (z, w) 的个数为 $\sum_{\alpha=0}^d p^\alpha_{ij} p^l_{k\alpha}$. 同理, 先计算 w 的个数, 然后计算 z 的个数, 就得到满足条件的 (z, w) 的个数为 $\sum_{\beta=0}^d p^\beta_{ki} p^l_{\beta j}$. 这就证明了 (vii) 成立. □

对于一个非对称的交换结合方案 $\mathfrak{X} = (X, \{R_i\}_{0\leqslant i\leqslant d})$, 我们可以把每个结合类 R_i 和对应的 $R_{i'}$ 合并, 记作 $\widetilde{R_i}$, 即

$$\widetilde{R_i} = R_i \cup R_{i'}.$$

设得到 d' 个非平凡类 $\widetilde{R_i}$, 这里 $\widetilde{R_0} = R_0$. 那么容易验证, $\widetilde{\mathfrak{X}} = (X, \{\widetilde{R_i}\}_{0\leqslant i\leqslant d'})$ 是一个对称结合方案.

实际上, 设 p^k_{ij} 是 $\mathfrak{X}$ 的交叉数, 而令 $\widetilde{p}^k_{ij}$ 是 $\widetilde{\mathfrak{X}}$ 的交叉数, 由命题 1.1(iv) 可知

$$\widetilde{p}^k_{ij} = p^k_{ij} + (1-\delta_{ii'})p^k_{i'j} + (1-\delta_{jj'})p^k_{ij'} + (1-\delta_{ii'})(1-\delta_{jj'})p^k_{i'j'}.$$

因此, $\widetilde{\mathfrak{X}} = (X, \{\widetilde{R_i}\}_{0\leqslant i\leqslant d'})$ 是一个对称结合方案. $\widetilde{\mathfrak{X}}$ 叫做 $\mathfrak{X}$ 的对称化(symmetrization).

设 $\mathfrak{X} = (X, \{R_i\}_{0\leqslant i\leqslant d})$ 是一个交换结合方案, 其类数为 d. 对于 $\mathfrak{X}$ 的每个结合关系 R_i 如下定义它的邻接矩阵 A_i, 其阶为 $|X| = n$, 它的行和列均用 X 的元素标记, (x, y) 位置上的元素定义为

$$(A_i)_{xy} = \begin{cases} 1, & \text{如果 } (x, y) \in R_i, \\ 0, & \text{不然}. \end{cases}$$

A_i 为 n 阶 $(0, 1)$ 矩阵. 易见, 结合方案定义中的条件 (i)~(v) 等价于下面的 (i)′~(v)′:

(i)′ $A_0 = I$ (单位矩阵);

(ii)′ $A_0 + A_1 + \cdots + A_d = J$ (全 1 矩阵);

(iii)′ ${}^tA_i = A_{i'}$, (A_i 的转置仍为一个邻接矩阵);

(iv)′ $A_iA_j = \sum_{k=0}^d p^k_{ij} A_k,\ i, j \in \{0, 1, \cdots, d\}$;

(v)′ $A_iA_j = A_jA_i,\ i, j \in \{0, 1, \cdots, d\}$.

这样, 如果给了 $d+1$ 个 n 阶 (0,1) 矩阵 $A_0, A_1, \cdots, A_d$ 满足条件 (i)$'$~ (v)$'$, 其中 p_{ij}^k 为非负整数, 那么就意味着存在一个交换结合方案 $\mathfrak{X}=(X, \{R_i\}_{0\leqslant i\leqslant d})$ 使得 $|X|=n$, 并且 A_i 恰为结合关系 R_i 的邻接矩阵, p_{ij}^k 为 $\mathfrak{X}$ 的交叉数.

设 $\mathfrak{X}=(X, \{R_i\}_{0\leqslant i\leqslant d})$ 是一个交换结合方案, $|X|=n$. 令 $M_n(\mathbb{C})$ 表示复数域 $\mathbb{C}$ 上的 n 阶全阵代数. 设 $A_0, A_1, \cdots, A_d$ 为 $\mathfrak{X}$ 的邻接矩阵. 由条件 (i)$'$~(v)$'$ 可知, 这组邻接矩阵在 $M_n(\mathbb{C})$ 中的 $\mathbb{C}$ 张成

$$\mathfrak{A}=\mathbb{C}A_0+\mathbb{C}A_1+\cdots+\mathbb{C}A_d$$

对于矩阵乘法是封闭的, 因而作成一个交换代数, 并且 $\dim_{\mathbb{C}}\mathfrak{A}=d+1$. 这个交换代数叫做结合方案 $\mathfrak{X}$ 的邻接代数, 或者 Bose-Mesner 代数.

由命题 1.1(iv) 可知, $\mathfrak{A}$ 的线性映射 $A_i\mapsto A_{i'}$ 给出 $\mathfrak{A}$ 的一个对合自同构. 考虑代数 $\mathfrak{A}$ 的左正则表示, 即每个元素 $A(\in\mathfrak{A})$ 左乘 $\mathfrak{A}$ 而给出 $\mathfrak{A}$ 的线性变换 $A: Y\mapsto AY$, 它在 $\mathfrak{A}$ 的基 $\{A_0, A_1, \cdots, A_d\}$ 之下对应一个 $d+1$ 阶矩阵. 设 $AA_j=\sum_{k=0}^d a_{jk}A_k$, $\mathbb{A}=(a_{jk})$, 那么 $A\mapsto {}^t\mathbb{A}$ 是 $\mathfrak{A}$ 到 $M_{d+1}(\mathbb{C})$ 内的一个代数同态. 由于 $\mathfrak{A}$ 有单位元, 这个同态是一个同构. 对于 $\mathfrak{A}$ 的基元素 A_i 来说, 由条件 (iv)$'$ 有

$$A_iA_j=\sum_{k=0}^d p_{ij}^k A_k.$$

我们令 B_i 为 $d+1$ 阶矩阵使得 $(B_i)_{jk}=p_{ij}^k$. 那么 A_i 的像为 ${}^tB_i$. 于是对应 $A_i\mapsto {}^tB_i\,(i=0,1,\cdots,d)$ 是 $\mathfrak{A}$ 到 $M_{d+1}(\mathbb{C})$ 中的一个同构. 因为 $\mathfrak{A}$ 是交换的, 所以 $A_i\mapsto B_i\,(i=0,1,\cdots,d)$ 给出 $\mathfrak{A}$ 到 $M_{d+1}(\mathbb{C})$ 的一个同构. 于是我们得到下面的

定理 1.2 设 $\mathfrak{X}=(X, \{R_i\}_{0\leqslant i\leqslant d})$ 是一个交换结合方案, 类数为 d, $A_0, A_1, \cdots, A_d$ 是它的邻接矩阵, $p_{ij}^k\,(i,j,k=0, 1, \cdots, d)$ 为交叉数. 再设 $\mathcal{B}$ 是 $M_{d+1}(\mathbb{C})$ 中由 $B_0, B_1, \cdots, B_d$ 张成的子代数. 那么 $\mathfrak{X}$ 的邻接代数 $\mathfrak{A}$ 在对应 $A_i\mapsto B_i$ 之下与 $\mathcal{B}$ 同构. 特别是, A_i 和 B_i 有相同的最小多项式.

$B_i=(p_{ij}^k)$ 叫做 $\mathfrak{X}$ 的第 i 个交叉矩阵, $\mathcal{B}$ 叫做 $\mathfrak{X}$ 的交叉代数. 交叉矩阵 $B_0, B_1, \cdots, B_d$ 满足下面的关系式

$${}^tB_i{}^tB_j=\sum_{k=0}^d p_{ij}^k\,{}^tB_k,\qquad i,j=0, 1, \cdots, d.$$

对于交换结合方案 $\mathfrak{X}$, 我们还有

$$B_iB_j=\sum_{k=0}^d p_{ij}^k B_k,\qquad i,j=0, 1, \cdots, d.$$

§1.2 例 子

我们给出结合方案的两个例子. 由于结合方案和群有着某种天然的联系, 我们就从一个群作用在一个集合上来开始.

例 1.1 设 G 是一个有限群, 可迁地作用在有限集合 Ω 上. 它自然地作用在 $\Omega\times\Omega$ 上, 即对于 $(x,\, y)\in\Omega\times\Omega$, $\sigma\in G$, 定义

$$(x,\, y)^\sigma=(x^\sigma,\, y^\sigma).$$

G 作用在 $\Omega\times\Omega$ 上不再是可迁的 (设 $|\Omega|=n>1$). 设有 $d+1$ 个轨道

$$\Lambda_0,\, \Lambda_1,\, \cdots,\, \Lambda_d,$$

其中 $\Lambda_0=\{(x,\, x)|x\in\Omega\}$ 是平凡轨道. 那么 $\mathfrak{X}=(\Omega,\, \{\Lambda_i\}_{0\leqslant i\leqslant d})$ 是一个结合方案 (不一定交换).

实际上, 结合方案定义中的条件 (i)~(iii) 显然成立. 现在看 (iv). 在轨道 Λ_k 中任取两个对子 $(x,\, y)$ 和 $(x',\, y')$, 那么, 存在元素 $\sigma\in G$ 使得 $x^\sigma=x'$ 及 $y^\sigma=y'$. 这样一来,

$$\{z'|(x',z')\in\Lambda_i,\, (z',y')\in\Lambda_j\}=\{z|(x,z)\in\Lambda_j,\, (z,x)\in\Lambda_j\}^\sigma.$$

由于 σ 作用在 Ω 上是一一的, 所以数 p_{ij}^k 与 Λ_k 中 (x,y) 的选取无关.

任取一个元素 $x\in\Omega$. 令

$$\Lambda_i(x)=\{y\in\Omega|(x,\, y)\in\Lambda_i\},$$

那么 $\Lambda_0(x)=\{x\}, \Lambda_1(x), \cdots, \Lambda_d(x)$ 恰为 x 的稳定子 G_x 在 Ω 上的轨道, 而价 $k_i=|\Lambda_i(x)|$.

现在, 考察这个结合方案的邻接代数. 令 $\mathbb{A}$ 为 G 在 Ω 上的置换表示. 就是说, 对每个元素 $\sigma\in G$, $\mathbb{A}(\sigma)$ 为如下定义的置换矩阵:

$$(\mathbb{A}(\sigma))_{xy}=\delta_{x^\sigma y}.$$

设 $|\Omega|=n$. 令 $\mathbb{A}(G)=\{\mathbb{A}(\sigma)|\sigma\in G\}\subset M_n(\mathbb{C})$, $\mathbb{A}$ 为 G 到 $\mathbb{A}(G)$ 上的一个群同态. 对于 $M_n(\mathbb{C})$ 中任一矩阵 $X=(X_{xy})$, 由于

$$(\mathbb{A}(\sigma)X\mathbb{A}(\sigma)^{-1})_{xy}=\sum_{s,t}\delta_{x^\sigma s}X_{st}\delta_{t^{\sigma^{-1}}y}=X_{x^\sigma y^\sigma},$$

可知 $X=(X_{xy})$ 与全体 $\mathbb{A}(\sigma)$ $(\sigma\in G)$ 交换当且仅当 $X_{xy}=X_{x^\sigma y^\sigma}$, 对所有 $\sigma\in G$. 注意到 $\mathfrak{X}$ 的邻接矩阵 A_i 满足这个条件, 并且 $A_0+A_1+\cdots+A_d=J$, 所以满足这个

条件的矩阵 X 必为 $A_0, A_1, \cdots, A_d$ 的线性组合. 因此, $\mathfrak{X}$ 的邻接代数 $\mathfrak{A}$ 恰为 $\mathbb{A}(G)$ 在 $M_n(\mathbb{C})$ 中的中心化子代数.

最后考虑 $\mathbb{A}(G)$ 的不可约表示直和分解, 再利用 Schur 引理可知, $\mathfrak{A}$ 是交换的当且仅当表示 $\mathbb{A}(G)$ 的不可约分支的重数均为 1.

我们得到下面的

定理 1.3　设有限群 G 可迁地作用在有限集合 Ω 上, $|\Omega| = n > 1$. (G, Ω) 自然地确定一个结合方案 $\mathfrak{X} = (\Omega, \{\Lambda_i\}_{0\leqslant i\leqslant d})$(不一定交换), 这里 $d+1$ 等于任一元素 $x \in \Omega$ 的稳定子 G_x 作用在 Ω 上的轨道数. $\mathfrak{X}$ 的邻接代数 $\mathfrak{A}$ 恰为 G 在 Ω 上的置换表示在 $M_n(\mathbb{C})$ 中的中心化子代数. $\mathfrak{X}$ 是交换的当且仅当这个置换表示的不可约分支的重数均为 1.

例 1.2　设 X 是一个有限群. 对于任一元素 $b \in X$, 它决定的右平移指的是 X 的一个置换 $t_b : x \longmapsto xb$, 全体右平移作成 X 上的一个置换群, 记作 $T(X)$. 显然 $T(X)$ 在 X 上是可迁的. 再设 G_0 是 X 的一个自同构群, 令 G 为 G_0 和 $T(X)$ 生成的群. 易见 $G = G_0 \cdot T(X)$ 为半直积, G 的每个元素可以唯一地表示成一个乘积 σt_b, $\sigma \in G_0$, $t_b \in T(X)$. 对于 $x \in X$, G 的元素 σt_b 作用 x 为

$$x^{\sigma t_b} = x^\sigma b.$$

显然, G 作用在 X 上是可迁的, 于是根据例 1.1, 确定 X 上的一个结合方案 $\mathfrak{X}$. 我们先考察这个结合方案的结合类的构成. 设 (x, y) 和 (x', y') 在同一个 G 轨道. 那么, 存在 G 中的元素 σt_b 使得 $(x, y)^{\sigma t_b} = (x', y')$, 即

$$x' = x^\sigma b, \quad y' = y^\sigma b.$$

于是有 $y'x'^{-1} = (yx^{-1})^\sigma$, 即 $y'x'^{-1}$ 与 yx^{-1} 在 X 的同一个 G_0 轨道. 反之, 如果两个对子 (x, y) 和 (x', y') 使得 yx^{-1} 和 $y'x'^{-1}$ 在同一个 G_0 轨道, 那么存在 $\sigma \in G_0$ 使得 $y'x'^{-1} = (yx^{-1})^\sigma = y^\sigma (x^\sigma)^{-1}$. 于是 $(y^\sigma)^{-1} y' = (x^\sigma)^{-1} x' = b$(设). 那么有 $x' = x^\sigma b$, $y' = y^\sigma b$, 即 $(x', y') = (x, y)^{\sigma t_b}$, 因而 (x, y) 和 (x', y') 在同一 G 轨道. 这样, 这个结合方案的结合类由 X 在 G_0 作用下的轨道决定. 设 $X_0 = \{1\}, X_1, \cdots, X_d$ 为 X 的全体 G_0 轨道, 那么这个结合方案的第 i 个结合类 R_i 为

$$R_i = \{(x, y) \in X \times X | yx^{-1} \in X_i\}.$$

$\mathfrak{X} = (X, \{R_i\}_{0\leqslant i\leqslant d})$, $d+1$ 为 X 的 G_0 轨道个数.

我们进一步考察这个结合方案的邻接代数. 设 $R = \mathbb{C}[X]$ 为群 X 在复数域 $\mathbb{C}$ 上的群环, 它是以 X 的元素作为基元素张成的 $\mathbb{C}$ 向量空间, 其中由 X 的群运算引入乘法所成的一个结合环. 对于每个 G_0 轨道 X_i, 令

$$\mathbb{X}_i = \sum_{x \in X_i} x, \quad i = 0, 1, \cdots, d.$$

$\mathbb{X}_0, \mathbb{X}_1, \cdots, \mathbb{X}_d$ 都是群环 $\mathbb{C}[X]$ 的元素. 按照 $\mathbb{C}[X]$ 中的乘法我们有

$$\mathbb{X}_i\mathbb{X}_j = \sum_{x\in X_i}\sum_{y\in X_j} xy.$$

易见, 如果上式右端的一个乘积 $xy = c$ 落在 G_0 轨道 X_k 中, 那么 X_k 中每个元 c' 必在上式右端的乘积项中出现, 而且与 c 出现的次数相同. 因此. 把这些乘积分组可设

$$\mathbb{X}_i\mathbb{X}_j = \sum_{k=0}^{d} c_{ij}^k \mathbb{X}_k, \tag{1.1}$$

这里 c_{ij}^k 为非负整数. 由 $\mathbb{X}_0, \mathbb{X}_1, \cdots, \mathbb{X}_d$ 生成的子代数记作 $\mathfrak{S}$, 叫做 X 上的一个Schur 环.

现在, 任取一个对子 $(x, y) \in R_k$, 即有 $yx^{-1} \in X_k$. 依结合方案定义有

$$p_{ij}^k = |\{z \in X | (x, z) \in R_i,\ (z, y) \in R_j\}|.$$

我们计算满足条件 $zx^{-1} \in X_i$ 和 $yz^{-1} \in X_j$ 之 z 的个数. 注意到 $yz^{-1} \cdot zx^{-1} = yx^{-1} \in X_k$, 由 (1.1) 恰有 c_{ij}^k 个对子 (a, b) 使得 $a \in X_i, b \in X_j$, 而 $ab = yx^{-1}$. 令 $z = a^{-1}y$, 那么 $yz^{-1} = a \in X_i$, $zx^{-1} = a^{-1}yx^{-1} = b \in X_j$, 即 $(x, z) \in R_j$, $(z, y) \in R_i$. 这样的对子 (a, b) 和 z 是一一对应的. 所以 $c_{ij}^k = p_{ji}^k$. 于是可知, $\mathfrak{X}$ 的邻接代数 $\mathfrak{A}$ 与 Schur 环 $\mathfrak{S}$ 反同构. 因此, $\mathfrak{X}$ 交换当且仅当 Schur 环 $\mathfrak{S}$ 是交换的. 特别地, $\mathfrak{X}$ 是对称的, 当且仅当每个 X_i 均为逆闭的, 即 $x \in X_i$ 当且仅当 $x^{-1} \in X_i$. 于是我们有

定理 1.4 设 X 是一个有限群, $T(X)$ 是 X 的右平移群. 再设 G_0 是 X 的一个自同构群, 并令 $G = \langle G_0, T(X)\rangle$. 那么 G 作用在 X 上是可迁的, 因而确定一个结合方案 $\mathfrak{X} = (X, \{R_i\}_{0\leqslant i\leqslant d})$, 其中 $d+1$ 为 X 的 G_0 轨道数. 设 $X_0 = \{1\}, X_1, \cdots, X_d$ 为 X 的 G_0 轨道, 在 X 的群环 $\mathbb{C}[X]$ 中由 $\mathbb{X}_i = \sum_{x\in X_i} x\,(i = 0, 1, \cdots, d)$ 生成的 Schur 环记作 $\mathfrak{S}$, 那么 $\mathfrak{X}$ 的邻接代数 $\mathfrak{A}$ 与 Schur 环 $\mathfrak{S}$ 反同构. $\mathfrak{X}$ 是交换的当且仅当 $\mathfrak{S}$ 是交换的. 特别地, $\mathfrak{X}$ 是对称的, 当且仅当每个 G_0 轨道 X_i 是逆闭的, 即 $x \in X_i$ 当且仅当 $x^{-1} \in X_i$.

推论 1.5 如果在定理 1.4 中我们取 G_0 为 X 的内自同构群, 那么所得结合方案 $\mathfrak{X} = (X, \{R_i\}_{0\leqslant i\leqslant d})$ 是交换的, 其中 $d+1$ 为 X 的共轭类个数. 这个结合方案叫做 X 的*群结合方案*(group association scheme).

证明 此时 G_0 轨道恰为群 X 的共轭类, 对于任 $a \in X$ 均有 $aX_ia^{-1} = X_i$ 即 $aX_i = X_ia$. 于是乘积 (1.1) 是交换的, 因而 $\mathfrak{X}$ 是交换的. □

推论 1.6 如果 X 本身就是一个交换群, 那么所得到的结合方案 $\mathfrak{X}$ 是交换的.

如果 X 是一个有限群, 而取 $G_0=\{1\}$ 即恒等自同构, 那么 $G=T(X)$, X 的平移群. 这时 X 的每个 G_0 轨道只包含一个元素. 设 X 的元素是 $x_0=e$ (X 的单位元), $x_1, \cdots, x_d$ ($|X|=d+1$). 这时, 结合方案 $\mathfrak{X}=(X, \{R_i\}_{0\leqslant i\leqslant d})$, 这里

$$R_i=\{(x,y)|yx^{-1}=x_i\},\ i=0,1,\cdots,d.$$

它的邻接代数就是 X 的群环 $\mathbb{C}[X]$.

§1.3　结合方案的特征值

我们讨论交换结合方案的特征值. 设 $\mathfrak{X}=(X, \{R_i\}_{0\leqslant i\leqslant d})$ 是一个类数为 d 的交换结合方案, $A_0, A_1, \cdots, A_d$ 是它的邻接矩阵, 它们在复数域 $\mathbb{C}$ 上张成 $\mathfrak{X}$ 的邻接代数 $\mathfrak{A}$, 它是全阵代数 $M_n(\mathbb{C})$ 的一个子代数, 这里 $n=|X|$.

邻接矩阵 A_i 的转置共轭还是一个邻接矩阵, 即 ${}^t\overline{A}_i=A_{i'}$, 而 A_i 与 $A_{i'}$ 交换, 所以 A_i 是正规矩阵. 这样, $A_0, A_1, \cdots, A_d$ 是 $d+1$ 个两两交换的正规矩阵. 从线性代数可知, 存在 n 阶酉矩阵 U ($U\,{}^t\overline{U}=I$) 使得 UA_iU^{-1} 同时化为对角阵, 设为

$$UA_iU^{-1}=[\alpha_{i1}, \alpha_{i2}, \cdots, \alpha_{in}],\ i=0,1,\cdots,d. \tag{1.2}$$

令 $V=\mathbb{C}^n$ 是 $\mathbb{C}$ 上 n 维行向量酉空间, $(x_1, \cdots, x_n)$ 和 $(y_1, \cdots, y_n)$ 的内积定义为 $x\cdot y=\sum_{i=1}^n x_i\overline{y}_i$. 我们仍用 X 的元素标记 n 阶矩阵的行和列, 并且标记 n 维行向量的分量. e_x 表示 x 分量为 1 而其余分量均为 0 的向量, $\{e_x|x\in X\}$ 是 V 的一组标准正交基. 由 (1.2) 有

$$UA_i=[\alpha_{i1}, \alpha_{i2}, \cdots, \alpha_{in}]U.$$

于是 U 的 n 个行向量都是 A_i ($i=0,1,\cdots,d$) 的公共特征向量. 因此我们可以将这 n 个公共特征向量适当分组生成若干个子空间, 而得到酉空间 V 的一个正交直和分解

$$V=V_0\perp V_1\perp\cdots\perp V_r,$$

使得 A_i 在 V_j 上特征值相同, 并且对于任一对 $i\neq j$, 存在 A_k 使得在 V_i 和 V_j 上的特征值不同. 注意到 $J=\sum_{i=0}^d A_i$ 的特征值为 n(1 重) 和 0 ($n-1$ 重), 因而属于 J 的特征值 n 的特征子空间是 1 维的, 显然它就是 $\langle(1, \cdots, 1)\rangle$. 另一方面, J 在每个 V_i 上的特征值相同. 因此, 必有某个 V_i, 比方说, $V_0=\langle(1, \cdots, 1)\rangle$.

现在, 令 E_i 是 V 到 V_i 上的正投影在标准正交基 $\{e_x|x\in X\}$ 下的矩阵, 那么有

$$E_0+E_1+\cdots+E_r=I \text{ 及 } E_iE_j=\delta_{ij}E_i.$$

E_0 是 V 到 $V_0=\langle(1,\cdots,1)\rangle$ 的正投影, 对于基向量 e_x 自然可设 $e_xE_0=\alpha_x(1,\cdots,1)$. 由于 $e_x-\alpha_x(1,\cdots,1)$ 和 $(1,\cdots,1)$ 正交, 立得 $1-n\alpha_x=0$, $\alpha_x=\frac{1}{n}$. 因此有

$$E_0=\frac{1}{n}J.$$

设 $\dim V_i=m_i$, 那么 $\mathrm{rank}E_i=m_i$. 再记 A_i 在 V_j 上的特征值为 $p_i(j)$, 那么我们有

$$A_i=\sum_{j=0}^{r}p_i(j)E_j. \tag{1.3}$$

因为 ${}^t\overline{E}_j=E_j$, 而 ${}^t\overline{A}_i=A_{i'}$, 所以我们有

$$p_{i'}(j)=\overline{p_i(j)}. \tag{1.4}$$

我们进一步断言: $r=d$. 由于 $E_0,E_1,\cdots,E_r$ 也是线性无关的, 所以只需证明每个 E_i 均可表为 $A_0,A_1,\cdots,A_d$ 的线性组合. 对于 $j\neq i$, 存在 A_{k_j} 使得 $p_{k_j}(j)\neq p_{k_j}(i)$. 令 $F_j=A_{k_j}-p_{k_j}(j)I$. 那么 F_j 在 V_i 上特征值为 $p_{k_j}(i)-p_{k_j}(j)\neq 0$, 而在 V_j 上为 0. 令 $F=\prod_{j\neq i}F_j$, 那么 F 在每个 $V_j\,(j\neq i)$ 上均为 0, 而在 V_i 上特征值不为 0, 因此 $F=\alpha E_i$, 对某个 $\alpha\neq 0$. 于是 E_i 可表为 $A_0,A_1,\cdots,A_d$ 的线性组合, 因而 $r=d$.

这样我们就证明了

定理 1.7 设 $\mathfrak{X}=(X,\{R_i\}_{0\leqslant i\leqslant d})$ 是一个交换结合方案, $A_0,A_1,\cdots,A_d$ 为 $\mathfrak{X}$ 的邻接矩阵. 那么酉空间 V 有正交直和分解 $V=V_0\perp V_1\perp\cdots\perp V_d$ 使得 V_i 为这些邻接矩阵的公共特征子空间, $V_0=\langle(1,\cdots,1)\rangle$. 又设 E_i 是 V 到 V_i 上的正投影在基 $\{e_x|x\in X\}$ 下的矩阵, 那么 $E_0,E_1,\cdots,E_d$ 恰为 $\mathfrak{X}$ 的邻接代数 $\mathfrak{A}$ 的本原幂等元.

数 $m_i=\dim V_i\,(i=0,1,\cdots,d)$ 叫做 $\mathfrak{X}$ 的**重数**.

由 (1.3) 我们有

$$A_i=\sum_{j=0}^{d}p_i(j)E_j,\ i=0,1,\cdots,d. \tag{1.5}$$

另一方面, $E_0,E_1,\cdots,E_d$ 也是邻接代数 $\mathfrak{A}$ 的一组基, 每个 E_i 可由 $A_0,A_1,\cdots,A_d$ 线性表出, 我们设

$$E_i=\frac{1}{|X|}\sum_{j=0}^{d}q_i(j)A_j,\ i=0,1,\cdots,d. \tag{1.6}$$

令

$$\begin{aligned}P&=(p_i(j)), &&\text{它的 }(j,i)\text{ 元素为 }p_i(j),\\ Q&=(q_i(j)), &&\text{它的 }(j,i)\text{ 元素为 }q_i(j).\end{aligned} \tag{1.7}$$

P 和 Q 都是 $d+1$ 阶矩阵, 它们分别称为交换结合方案 $\mathfrak{X}$ 的第一特征值矩阵 和第二特征值矩阵. 显然有下面的关系式

$$PQ = QP = |X|I.$$

现在, 我们引入矩阵的 Hadamard 乘法. 设 A 和 B 是两个大小相同的矩阵, A 和 B 的Hadamard 乘积定义为由 A 与 B 对应元素之积作为相应位置上的元素所成的矩阵, 记作 $A \circ B$. $\mathfrak{X}$ 的邻接矩阵 $A_0, A_1, \cdots, A_d$ 满足下面的关系式

$$A_0 + A_1 + \cdots + A_d = J, \quad A_i \circ A_j = \delta_{ij} A_i. \tag{1.8}$$

我们再引入一个符号, 对任意矩阵 C, 令 $\tau(C)$ 表示 C 的全体元素之和. 直接计算可知下面的等式成立

$$tr(A\,{}^tB) = tr({}^tAB) = \tau(A \circ B), \tag{1.9}$$

这里 $\mathrm{tr}(C)$ 表示矩阵 C 的迹 (trace).

容易看出, 我们有

$$\mathrm{tr}(A_i) = |X|\delta_{i0}, \ \ \mathrm{tr}(E_i) = m_i, \tag{1.10}$$

$$\tau(A_i) = |X|k_i, \ \ \tau(E_i) = |X|\delta_{i0}. \tag{1.11}$$

这里我们来看最后一个等式. 注意到 $E_0 = \frac{1}{|X|}J$, 所以 $\tau(E_0) = |X|$. 而对于 $i \neq 0$, 由于 $0 = E_0E_i$, 利用 (1.9) 可得

$$0 = \mathrm{tr}(E_0E_i) = \tau({}^tE_0 \circ E_i) = \tau\left(\frac{1}{|X|}J \circ E_i\right) = \frac{1}{|X|}\tau(E_i).$$

我们对 $\mathfrak{X}$ 的特征值矩阵作进一步的考察. 我们有

命题 1.8　对于每个 $i\,(i = 0, 1, \cdots, d)$, 有

(i) $p_0(i) = 1, \ p_i(0) = k_i$,

(ii) $q_0(i) = 1, \ q_i(0) = m_i$.

证明　比较 A_0 的两个等式 $A_0 = \sum_{i=0}^{d} p_0(i)E_i$ 和 $A_0 = I = E_0 + E_1 + \cdots + E_d$ 立得 $p_0(i) = 1$. 比较 E_0 的两个等式 $E_0 = \frac{1}{|X|}\sum_{i=0}^{d} q_0(i)A_i$ 和 $E_0 = \frac{1}{|X|}J = \frac{1}{|X|}(A_0 + A_1 + \cdots + A_d)$ 立得 $q_0(i) = 1$. 用 τ 作用 (1.5), 并利用 (1.11) 就有

$$|X|k_i = \tau(A_i) = \sum_{j=0}^{d} p_i(j)\tau(E_j) = p_i(0)|X|.$$

于是得 $p_i(0) = k_i$. 用 tr 作用 (1.6), 并利用 (1.10) 就可得 $q_i(0) = m_i$. □

因此, P 和 Q 具有下面的形状

$$P=\begin{pmatrix}1 & k_1 & \cdots & k_d\\ 1 & & & \\ \vdots & & p_i(j) & \\ 1 & & & \end{pmatrix},\qquad Q=\begin{pmatrix}1 & m_1 & \cdots & m_d\\ 1 & & & \\ \vdots & & q_i(j) & \\ 1 & & & \end{pmatrix}.$$

进一步我们有

定理 1.9 设 $P=(p_i(j))$ 和 $Q=(q_i(j))$ 分别是交换结合方案 $\mathfrak{X}$ 的第一特征值矩阵和第二特征值矩阵. 那么有下面的等式

$$q_j(i)k_i=\overline{p_i(j)}m_j,\ i,j=0,1,\cdots,d.$$

写成矩阵形式就是

$$[k_0,k_1,\cdots,k_d]Q={}^t\overline{P}[m_0,m_1,\cdots,m_d].$$

证明 注意到

$$A_i\circ E_j=\frac{1}{|X|}q_j(i)A_i.$$

用 τ 作用得 $\tau(A_i\circ E_j)=q_j(i)k_i$. 另一方面, 利用 (1.9) 又可得

$$\tau(A_i\circ E_j)=tr(A_{i'}E_j)=tr(p_{i'}(j)E_j)=p_{i'}(j)m_j.$$

再利用 (1.4) 立得 $q_j(i)k_i=\overline{p_i(j)}m_j$. □

利用关系式 $PQ=QP=|X|I$ 和定理 1.9 就得到

定理 1.10 交换结合方案 $\mathfrak{X}$ 的特征值 $p_i(j)$ 满足下面的正交关系:

(i) 第一正交关系 $\sum_{\nu=0}^{d}\frac{1}{k_\nu}p_\nu(i)\overline{p_\nu(j)}=\frac{|X|}{m_i}\delta_{ij}$, (1.12)

(ii) 第二正交关系 $\sum_{\nu=0}^{d}m_\nu p_i(\nu)\overline{p_j(\nu)}=|X|k_i\delta_{ij}$. (1.13)

在特征值的第一正交关系 (1.12) 中令 $j=i$ 就得到下面的重数公式

$$m_i=|X|\Big/\sum_{\nu=0}^{d}\frac{1}{k_\nu}p_\nu(i)\overline{p}_\nu(i).\tag{1.14}$$

由关系式 (1.14) 知, 交换结合方案 $\mathfrak{X}$ 的重数由第一特征值矩阵 P 所确定. 又从 (1.5) 知, P 是邻接代数 $\mathfrak{A}$ 的基 $A_0,A_1,\cdots,A_d$ 到基 $E_0,E_1,\cdots,E_d$ 的转换矩阵, $\mathfrak{A}$ 的这些本原幂等元是唯一的, 所以 P 由 $\mathfrak{A}$ 唯一确定, A_i 和 E_j 的顺序仅引起 P 的列和行的置换, 不过我们要求 P 有上面给出的形状.

又从定理 1.2 知, $\mathfrak{X}$ 的邻接代数 $\mathfrak{A}$ 和它的交叉代数 $\mathfrak{B}$ 同构, 所以 P 也应由 $\mathfrak{X}$ 的交叉矩阵 $B_0,B_1,\cdots,B_d$ 所确定. 实际上, 由于 A_i 的左正则表示在基

$A_0, A_1, \cdots, A_d$ 之下的矩阵为 ${}^tB_i$; 而在基 $E_0, E_1, \cdots, E_d$ 之下的矩阵为对角阵 $[p_i(0), p_i(1), \cdots, p_i(d)]$, 转换矩阵为 P, 所以自然有

$$ {}^tB_i = P^{-1}[(p_i(0), p_i(1), \cdots, p_i(d))]P, $$

左乘 P 就得

$$ P\,{}^tB_i = [p_i(0), p_i(1), \cdots, p_i(d)]P. \tag{1.15} $$

这就是说, P 的行向量均为 ${}^tB_0, {}^tB_1, \cdots, {}^tB_d$ 的公共特征向量, 当然, 它们的第一分量都归一化了.

对 (1.15) 的两端取 (α, j) 元素得

$$ p_i(\alpha)p_j(\alpha) = \sum_{k=0}^{d} p_{ij}^k p_k(\alpha). \tag{1.16} $$

由此可知, 对于每个 $\alpha \in \{0, 1, \cdots, d\}$ 线性映射

$$ \delta_\alpha : A_i \longrightarrow p_i(\alpha), \quad i = 0, 1, \cdots, d $$

是邻接代数 $\mathfrak{A}$ 关于基 $A_0, \cdots, A_d$ 的线性表示. 进一步, 可以证明, $\mathfrak{A}$ 关于基 $A_0, \cdots, A_d$ 的任一线性表示必为某个 δ_α([2] Cha II. Proposition 5.4).

最后, 我们给出有限群 G 的群结合方案的特征值矩阵 P 和 G 的特征标表 (character table) T 的关系 (这里需要关于群特征标的一些知识).

设 G 是一个有限群, $C_0 = \{e\}, C_1, \cdots, C_d$ 是 G 的全体共轭类. 令

$$ R_i = \{(x, y) \in G \times G | yx^{-1} \in C_i\}, i = 0, \cdots, d. $$

由推论 1.5 知, $\mathfrak{X} = (G, \{R_i\}_{0 \leqslant i \leqslant d})$ 是 G 上的一个交换结合方案, 叫做 G 的群结合方案. 这时, R_i 的价 $k_i = |C_i|, i = 0, 1, \cdots, d$.

另一方面, 由特征标理论可知, G 恰有 $d+1$ 个不等价的不可约特征标, 记作 $\chi_0 = 1$(单位特征标), $\chi_1, \cdots, \chi_d$. 令 $a_0 = e, a_1, \cdots, a_d$ 是 G 的共轭类的一个代表系 (即 $a_i \in C_i$). G 的特征标表指的是如下 $d+1$ 阶的矩阵 T, 它的 (α, i) 元素为 $\chi_\alpha(a_i)$:

$$ T = (\chi_\alpha(a_i)), $$

$\chi_0(a_i) = 1, i = 0, 1, \cdots, d$; $\chi_\alpha(a_0) = \chi_\alpha(e)$ 为不可约特征标 χ_α 的级 (degree).

令 $\mathbb{C}_i = \sum_{x \in C_i} x$ (群环 $\mathbb{C}[G]$ 中的元素), 那么有

$$ \mathbb{C}_i\mathbb{C}_j = \sum_{k=0}^{d} p_{ij}^k \mathbb{C}_k, $$

p_{ij}^k 也是群结合方案 $\mathfrak{X}$ 的交叉数. 现在设 χ 为 G 的一个不可约特征标, 令 $w_i = k_i\chi(a_i)/\chi(e)$, 可以证明, 线性映射

$$\Delta : A_i \longrightarrow w_i \quad (i = 0, 1, \cdots, d)$$

是群结合方案 $\mathfrak{X}$ 的邻接代数 $\mathfrak{A}$ 对于基 $A_0, A_1, \cdots, A_d$ 的一个线性表示. 因此, 它必为 $\mathfrak{A}$ 的某个线性表示

$$\delta_\alpha : A_i \longrightarrow p_i(\alpha) \quad (i = 0, 1, \cdots, d).$$

于是适当排列 $\chi_1, \cdots, \chi_d$ 的顺序, 我们可设

$$\frac{k_i\chi_\alpha(a_i)}{\chi_\alpha(e)} = p_i(\alpha), \quad i, \alpha = 0, 1, \cdots, d,$$

即有

$$\left[\frac{1}{\chi_0(e)}, \cdots, \frac{1}{\chi_d(e)}\right] T[k_0, \cdots, k_d] = P. \tag{1.17}$$

再由群特征标的第一正交关系可以导出 $\chi_\alpha(e) = \sqrt{m_\alpha}$, 这里 m_α 是群结合方案 $\mathfrak{X}$ 的重数. 详细讨论, 请参阅 [2] 的 II.7.

§1.4 Krein 参数

从 (1.8) 知, 交换结合方案 $\mathfrak{X}$ 的邻接代数 $\mathfrak{A}$ 中矩阵的 Hadamard 乘法也是封闭的. 关于 Hadamard 乘法下的这个代数叫做 $\mathfrak{A}$ 的对偶代数, 记作 $\widehat{\mathfrak{A}}$. 对于代数 $\widehat{\mathfrak{A}}$ 来说, J 是它的单位元, $A_0, A_1, \cdots, A_d$ 是 $\widehat{\mathfrak{A}}$ 的本原幂等元. 由于 $E_i \circ E_j$ 也是 $E_0, E_1, \cdots, E_d$ 的线性组合, 我们设

$$E_i \circ E_j = \frac{1}{|X|}\sum_{k=0}^{d} q_{ij}^k E_k, \ i, j = 0, 1, \cdots, d. \tag{1.18}$$

系数 q_{ij}^k 叫做 $\mathfrak{X}$ 的Krein 参数.

首先我们有

定理 1.11 交换结合方案 $\mathfrak{X} = (X, \{R_i\}_{0\leqslant i\leqslant d})$ 的 Krein 参数 q_{ij}^k 都是非负实数.

证明 用 E_k 左乘等式 (1.18) 的两端, 得

$$E_k(E_i \circ E_j) = \frac{1}{|X|} q_{ij}^k E_k.$$

由此可知 $\frac{1}{|X|} q_{ij}^k$ 为矩阵 $E_i \circ E_j$ 的一个特征值. 我们知道, E_i 和 E_j 都是半正定 Hermite 矩阵, 所以二者的 Kroneker 积 $E_i \otimes E_j$ 也是半正定的, 因而它的每个主子矩

阵都是半正定的. 现在 $E_i \circ E_j$ 是 $E_i \otimes E_j$ 的一个主子矩阵, 所以是半正定 Hermite 矩阵, 从而它的特征值是非负实数. 于是有 $q_{ij}^k \geqslant 0$. □

注意到交换邻接代数 $\mathfrak{A}$ 的本原幂等元组是唯一的, 而 ${}^tE_0, {}^tE_1, \cdots, {}^tE_d$ 也是 $\mathfrak{A}$ 的本原幂等元, 所以

$${}^tE_i = E_{\hat{i}}, \text{对某个} \hat{i} \in \{0, 1, \cdots, d\}.$$

再由 ${}^tE_i = \overline{E}_i$ 和 (1.6) 可得

$$q_{\hat{i}}(j) = \overline{q_i(j)}.$$

定理 1.12 对于 Krein 参数和特征值之间的关系, 我们有

(i)

$$\begin{aligned} q_{ij}^k &= \frac{1}{|X|m_k} \sum_{\nu=0}^{d} k_\nu q_i(\nu) q_j(\nu) \overline{q_k(\nu)} \\ &= \frac{m_i m_j}{|X|} \sum_{\nu=0}^{d} \frac{1}{k_\nu^2} p_\nu(i) p_\nu(j) \overline{p_\nu(k)}. \end{aligned}$$

(ii)

$$\begin{aligned} p_{ij}^k &= \frac{1}{|X|k_k} \sum_{\nu=0}^{d} m_\nu p_i(\nu) p_j(\nu) \overline{p_k(\nu)} \\ &= \frac{k_i k_j}{|X|} \sum_{\nu=0}^{d} \frac{1}{m_\nu^2} q_\nu(i) q_\nu(j) \overline{q_\nu(k)}. \end{aligned}$$

证明 (i) 从 (1.18) 可得

$$\frac{1}{|X|} q_{ij}^k E_k = (E_i \circ E_j) E_k.$$

对这个等式取 trace, 有

$$\begin{aligned} \frac{1}{|X|} q_{ij}^k m_k &= tr((E_i \circ E_j)E_k) = \tau(E_i \circ E_j \circ {}^tE_k) \\ &= \tau(E_i \circ E_j \circ E_{\hat{k}}) \\ &= \tau\left(\frac{1}{|X|^3} \sum_{\nu=0}^{d} q_i(\nu) q_j(\nu) q_{\hat{k}}(\nu) A_\nu\right) \\ &= \frac{1}{|X|^2} \sum_{\nu=0}^{d} q_i(\nu) q_j(\nu) q_{\hat{k}}(\nu) k_\nu \\ &= \frac{1}{|X|^2} \sum_{\nu=0}^{d} q_i(\nu) q_j(\nu) \overline{q_k(\nu)} k_\nu \\ &= \frac{m_i m_j m_k}{|X|^2} \sum_{\nu=0}^{d} \frac{1}{k_\nu^2} \overline{p_\nu(i)}\, \overline{p_\nu(j)} p_\nu(k). \end{aligned}$$

因为 $\overline{p_\nu(i)} = p_{\nu'}(i)$, $k_\nu = k_{\nu'}$, 所以从上式又得

$$\frac{1}{|X|} q_{ij}^k m_k = \frac{m_i m_j m_k}{|X|^2} \sum_{\nu=0}^{d} \frac{1}{k_\nu^2} p_\nu(i) p_\nu(j) \overline{p_\nu(k)}.$$

由此立得 (i).

(ii) 应用 τ 于

$$p_{ij}^k A_k = (A_i A_j) \circ A_k,$$

那么有

$$\begin{aligned} p_{ij}^k |X| k_k &= \tau((A_i A_j) \circ A_k) = tr(A_i A_j A_{k'}) \\ &= tr\left(\sum_{\nu=0}^{d} p_i(\nu) p_j(\nu) p_{k'}(\nu) E_\nu\right) \\ &= \sum_{\nu=0}^{d} p_i(\nu) p_j(\nu) \overline{p_k(\nu)} m_\nu \\ &= k_i k_j k_k \sum_{\nu=0}^{d} \frac{1}{m_\nu^2} \overline{q_\nu(i)}\, \overline{q_\nu(j)} q_\nu(k). \end{aligned}$$

因为 p_{ij}^k 为实数, 两边取共轭就可得 (ii). □

类似于命题 1.1 中 p_{ij}^k 的关系式, 我们有

命题 1.13 Krein 参数 q_{ij}^k 满足如下关系式:

(i) $q_{0j}^k = \delta_{jk}$,

(ii) $q_{i0}^k = \delta_{ik}$,

(iii) $q_{ij}^0 = m_i \delta_{i\hat{j}}$,

(iv) $q_{ij}^k = q_{\hat{i}\hat{j}}^{\hat{i}}$,

(v) $\sum_{j=0}^{d} q_{ij}^k = m_i$,

(vi) $m_k q_{ij}^k = m_j q_{\hat{i}k}^j = m_i q_{k\hat{j}}^i$,

(vii) $\sum_{\alpha=0}^{d} q_{ij}^\alpha q_{k\alpha}^l = \sum_{\beta=0}^{d} q_{ki}^\beta q_{\beta j}^l$.

证明 (i) 比较下面的等式

$$E_0 \circ E_j = \frac{1}{|X|} \sum_{k=0}^{d} q_{0j}^k E_k \text{ 和 } E_0 \circ E_j = \frac{1}{|X|} J \circ E_j = \frac{1}{|X|} E_j.$$

立得 (i).

(ii) 由 $E_i \circ E_j = E_j \circ E_i$ 推出 $q_{ij}^k = q_{ji}^k$. 特别 $q_{i0}^k = q_{0i}^k = \delta_{ik}$.

(iii) 利用 (1.18) 可得 $q_{ij}^0 E_0 = |X|(E_i \circ E_j)E_0$, 再取 trace, 有

$$\begin{aligned} q_{ij}^0 &= |X|\tau(E_i \circ E_j \circ E_0) = \tau(E_i \circ E_j) = tr(E_i E_{\widehat{j}}) \\ &= tr(\delta_{i\widehat{j}} E_i) = m_i \delta_{i\widehat{j}}. \end{aligned}$$

(iv) 对 (1.18) 两边取转置, 有

$${}^t(E_i \circ E_j) = \frac{1}{|X|}\sum_{k=0}^{d} q_{ij}^k E_{\widehat{k}}.$$

另一方面,

$${}^t(E_i \circ E_j) = E_{\widehat{i}} \circ E_{\widehat{j}} = \frac{1}{|X|}\sum_{k=0}^{d} q_{\widehat{i}\widehat{j}}^{\widehat{k}} E_{\widehat{k}}.$$

比较系数立得 $q_{ij}^k = q_{\widehat{i}\widehat{j}}^{\widehat{k}}$.

(v) 计算

$$\begin{aligned} \sum_{j=0}^{d}(E_i \circ E_j) &= E_i \circ \left(\sum_{j=0}^{d} E_j\right) = E_i \circ I = \left(\frac{1}{|X|}\sum_{\nu=0}^{d} q_i(\nu)A_\nu\right) \circ A_0 \\ &= \frac{1}{|X|} q_i(0) A_0 \\ &= \frac{1}{|X|} m_i \sum_{k=0}^{d} E_k. \end{aligned}$$

另一方面,

$$\sum_{j=0}^{d}(E_i \circ E_j) = \sum_{j=0}^{d}\frac{1}{|X|}\sum_{k=0}^{d} q_{ij}^k E_k = \sum_{k=0}^{d}\left(\frac{1}{|X|}\sum_{j=0}^{d} q_{ij}^k\right) E_k.$$

比较 E_k 的系数立得 (v).

(vi) 由定理 1.12(i) 的证明可知 $\tau(E_i \circ E_j \circ E_{\widehat{k}}) = \frac{1}{|X|} q_{ij}^k m_k$ 为实数, 取复共轭有

$$\tau(E_i \circ E_j \circ E_{\widehat{k}}) = \tau(E_{\widehat{i}} \circ E_k \circ E_{\widehat{j}}) = \tau(E_k \circ E_{\widehat{j}} \circ E_{\widehat{i}}).$$

于是有

$$\frac{m_k}{|X|} q_{ij}^k = \frac{m_j}{|X|} q_{\widehat{i}k}^j = \frac{m_i}{|X|} q_{k\widehat{j}}^i,$$

从而立得 (vi).

(vii) 由 Hadamard 乘积的结合性, 有

$$E_k \circ (E_i \circ E_j) = (E_k \circ E_i) \circ E_j.$$

现在

$$左边 = E_k \circ \left(\frac{1}{|X|}\sum_{\alpha=0}^{d} q_{ij}^{\alpha} E_{\alpha}\right) = \frac{1}{|X|^2}\sum_{l=0}^{d}\left(\sum_{\alpha=0}^{d} q_{ij}^{\alpha} q_{k\alpha}^{l}\right) E_l,$$

$$右边 = \left(\frac{1}{|X|}\sum_{\beta=0}^{d} q_{ki}^{\beta} E_{\beta}\right) \circ E_j = \frac{1}{|X|^2}\sum_{l=0}^{d}\left(\sum_{\beta=0}^{d} q_{ki}^{\beta} q_{\beta j}^{l}\right) E_l.$$

比较 E_l 的系数立得 (vii). □

我们令 $\widehat{B}_i = (q_{ij}^k)$, 它的 (j, k) 位置元素为 q_{ij}^k. 注意到, 由 (1.18) 可得

$$(|X|E_i) \circ (|X|E_j) = \sum_{k=0}^{d} q_{ij}^k (|X|E_k).$$

而由 (1.6) 可得

$$(|X|E_i) \circ A_j = q_i(j) A_j.$$

于是考虑 $|X|E_i$ 在 $\widehat{\mathfrak{A}}$ 中的乘法分别在基 $|X|E_0, |X|E_1, \cdots, |X|E_d$ 和 A_0, $A_1, \cdots$, A_d 之下的矩阵, 立得

$$Q\,{}^t\widehat{B}_i = [q_i(0), q_i(1), \cdots, q_i(d)]Q, \tag{1.19}$$

因而第二特征矩阵 Q 的行向量恰为 ${}^t\widehat{B}_0, {}^t\widehat{B}_1, \cdots, {}^t\widehat{B}_d$ 的公共特征向量, 其第一分量归一化了.

定理 1.12 和 (1.15) 及 (1.19) 说明了交换结合方案 $\mathfrak{X}$ 的特征值矩阵 P, Q 和它的交叉数 p_{ij}^k 及 Krein 参数 q_{ij}^k 之间的关系, 又从命题 1.13 看到 Krein 参数 q_{ij}^k 表现的就像是某个结合方案的交叉数. 现在, 我们给出对偶结合方案的概念.

设 $\mathfrak{X} = (X, \{R_i\}_{0 \leqslant i \leqslant d})$ 和 $\mathfrak{Y} = (Y, \{W_i\}_{0 \leqslant i \leqslant d})$ 是两个交换结合方案, 类数均为 d, 并且 $|X| = |Y|$. 如果 $\mathfrak{X}$ 的 Krein 参数恰和 $\mathfrak{Y}$ 的交叉数一致, 或者等价地, $\mathfrak{X}$ 的第二特征值矩阵恰和 $\mathfrak{Y}$ 的第一特征值矩阵一致, 那么, 就称 $\mathfrak{X}$ 和 $\mathfrak{Y}$ 是*形式对偶的*(formally dual).

如果 $\mathfrak{X}$ 的交叉数和它自己的 Krein 参数一致, 或者等价地, $\mathfrak{X}$ 的第一特征值矩阵和它的第二特征值矩阵一致, 那么就称 $\mathfrak{X}$ 是*自对偶的*(self dual).

§1.5 有限交换群上 S 环的对偶性

在这一节中我们要证明, 如果 X 是一个有限交换群, 那么对于定理 1.4 中给出的交换结合方案, 或更一般地说, 对于 X 上的一个 S 环决定的结合方案 $\mathfrak{X}$, 存在结合方案 $\mathfrak{Y}$ 与 $\mathfrak{X}$ 成形式对偶. 我们从 S 环谈起.

设 X 是一个有限群, $X_0, X_1, \cdots, X_d$ 是 X 的非空子集而具有下面的性质:

(i) $X = X_0 \cup X_1 \cup \cdots \cup X_d$, $X_i \cap X_j = \varnothing (i \neq j)$,

(ii) $X_0 = \{1\}$ (群 X 的单位元),

(iii) 令 $X_i^{-1} = \{x^{-1} | x \in X_i\}$, 那么 $X_i^{-1} = X_{i'}$ 对某个 i',

(iv) 记 $\mathbb{X}_i = \sum_{x \in X_i} x$, 那么

$$\mathbb{X}_i \mathbb{X}_j = \sum_{k=0}^{d} c_{ij}^k \mathbb{X}_k.$$

((iv) 自然蕴含 c_{ij}^k 为非负整数). 注意到定理 1.4 中的那些 G_0 轨道就具有这些性质. 令 $\mathbb{C}[X]$ 表示 X 在复数域上的群环, $\mathbb{X}_i$ 为 $\mathbb{C}[X]$ 中的元素. 令 $\mathfrak{S}$ 为 $\mathbb{C}[X]$ 中由 $\mathbb{X}_0, \mathbb{X}_1, \cdots, \mathbb{X}_d$ 生成的子代数, 叫做 X 上的一个 S 环 (Schur 环). 容易看出 $\dim \mathfrak{S} = d + 1$.

对于 X 上的 S 环 $\mathfrak{S}$, 如下定义 X 上的关系 R_i:

$$R_i = \{(x, y) | yx^{-1} \in X_i\}, \qquad i = 0, 1, \cdots, d.$$

注意到 X 的右平移保持 R_i 不变, 性质 (i)~(iv) 意味着 $\mathfrak{X} = (X, \{R_i\}_{0 \leqslant i \leqslant d})$ 是一个结合方案, 叫做由 $\mathfrak{S}$ 决定的结合方案, 记作 $\mathfrak{X}(\mathfrak{S})$.

令 A_i 为关系 R_i 的邻接矩阵, 即 $(A_i)_{xy} = 1$ 当且仅当 $yx^{-1} \in X_i$. $\mathfrak{X}(\mathfrak{S})$ 的交叉数 p_{ij}^k 使 $A_i A_j = \sum_{k=0}^{d} p_{ij}^k A_k$. 易见, $p_{ij}^k = c_{ji}^k$. 所以映射 $A_i \mapsto \mathbb{X}_i$ 给出 $\mathfrak{X}(\mathfrak{S})$ 的邻接代数 $\mathfrak{A}$ 到 $\mathfrak{S}$ 的一个反同构. 如果 X 是交换的, 那么 $\mathfrak{S}$ 是交换的, 因而 $\mathfrak{X}(\mathfrak{S})$ 是交换的 (参看定理 1.4).

以下设 X 是一个有限交换群, $\mathfrak{S} = \langle \mathbb{X}_0, \mathbb{X}_1, \cdots, \mathbb{X}_d \rangle$ 是 X 上的一个 S 环, 我们要证明存在结合方案 $\mathfrak{Y}$ 与 $\mathfrak{X}(\mathfrak{S})$ 成形式对偶.

为此, 我们考虑 X 的群环 $\mathbb{C}[X]$, 它也是 X 上的一个 S 环. 实际上, 设 $|X| = n$, X 中的元素记作 $x_0 = 1$(单位元), $x_1, \cdots, x_{n-1}$. 我们把 X 上的一元子集 $\{x_i\}$ 记作 $\underline{X}_i$, 那么 $\underline{X}_0, \underline{X}_1, \cdots, \underline{X}_{n-1}$ 具有上面的性质 (i)~(iv), 因而得到一个 S 环, 它就是群环 $\mathbb{C}[X]$. 注意到 $x_i^{-1} = x_{i'}$.

由 S 环 $\mathbb{C}[X]$ 决定的交换结合方案记作 $\underline{\mathfrak{X}} = \mathfrak{X}(\mathbb{C}[X])$, 它的结合关系

$$\underline{R}_i = \{(x, y) | yx^{-1} = x_i\}, \ i = 0, 1, \cdots, n-1.$$

$\underline{R}_i$ 的邻接矩阵 $\underline{A}_i$ 的元素

$$(\underline{A}_i)_{xy} = \begin{cases} 1, & \text{如果 } x_i x = y, \\ 0, & \text{不然}. \end{cases}$$

显然, 它是 X 的正则表示下 x_i 给出的置换矩阵 (注意 X 是交换群).

令 $\mathfrak{A}$ 表示 $\mathfrak{X}$ 的邻接代数, 那么映射 $\underline{f}: \underline{A}_i \mapsto x_i$ 给出 $\mathfrak{A}$ 到 $\mathbb{C}[X]$ 的一个同构. 记 $\mathfrak{X}$ 的交叉数为 $\underline{p}_{ij}^k$. 如果 $x_ix_j = x_k$, 那么有 $\underline{A}_i\underline{A}_j = \underline{A}_k$, 因而交叉数 $\underline{p}_{ij}^0, \underline{p}_{ij}^1, \cdots, \underline{p}_{ij}^{n-1}$ 中有且仅有一个为 1, 其余的均为 0, 即

$$\underline{p}_{ij}^k = \begin{cases} 1, & \text{如果 } x_ix_j = x_k, \\ 0, & \text{不然}. \end{cases}$$

于是, 交叉矩阵 $\underline{B}_i = \underline{A}_i$. 又 $\mathfrak{X}$ 的价 $\underline{k}_i = 1$, 并且重数 $\underline{m}_i = 1, i = 0, 1, \cdots, n-1$.

设邻接代数 $\mathfrak{A}$ 的本原幂等元为 $\underline{E}_0, \underline{E}_1, \cdots, \underline{E}_{n-1}$, 并设

$$\underline{A}_i = \sum_{j=0}^{n-1} \underline{p}_i(j)\underline{E}_j,$$

$$\underline{E}_i = \frac{1}{n}\sum_{j=0}^{n-1} \underline{q}_i(j)\underline{A}_j,$$

即 $\mathfrak{X}$ 的特征值为 $\underline{p}_i(j)$. 它的第一和第二特征值矩阵分别记作 $\underline{P}$ 和 $\underline{Q}$, 即 $\underline{P}(\underline{p}_i(j))$, $\underline{Q} = (\underline{q}_i(j))$, 并且 $\underline{P}\underline{Q} = \underline{Q}\underline{P} = nI$.(注意, 这时, $\underline{P}$ 就是交换群 X 的特征标表.)

再设 $e_i = \underline{f}(\underline{E}_i) \in \mathbb{C}[X]$. 那么 $e_0, e_1, \cdots, e_{n-1}$ 为 $\mathbb{C}[X]$ 的本原幂等元, 并且

$$x_i = \sum_{j=0}^{n-1} \underline{p}_i(j)e_j.$$

$$e_i = \frac{1}{n}\sum_{j=0}^{n-1} \underline{q}_i(j)x_j.$$

$\mathfrak{A}$ 在 Hadamard 乘法下封闭, $\underline{A}_i \circ \underline{A}_j = \delta_{ij}\underline{A}_i$. 设

$$(n\underline{E}_i) \circ (n\underline{E}_j) = \sum_{k=0}^{n-1} \underline{q}_{ij}^k(n\underline{E}_k), \tag{1.20}$$

这里 $\underline{q}_{ij}^k$ 是 $\mathfrak{X}$ 的 Krein 参数. 对应地, 我们在 $\mathbb{C}[X]$ 中定义 Hadamard 乘法: $x_i \circ x_j = \delta_{ij}x_i$. $\mathbb{C}[X]$ 关于 Hadamard 乘法作成的代数记作 $\mathbb{C}[X]^*$, $\underline{f}$ 也是 $\widehat{\mathfrak{A}}$ ($\mathfrak{A}$ 的对偶代数) 到 $\mathbb{C}[X]^*$ 的同构. 于是我们有

$$(ne_i) \circ (ne_j) = \sum_{k=0}^{n-1} \underline{q}_{ij}^k(ne_k). \tag{1.20$'$}$$

现在回到 S 环 $\mathfrak{S} = \langle \mathbb{X}_0, \mathbb{X}_1, \cdots, \mathbb{X}_d \rangle$, 它是 $\mathbb{C}[X]$ 的一个子代数, 并且由于

$$\mathbb{X}_i \circ \mathbb{X}_j = \left(\sum_{x \in X_i} x\right) \circ \left(\sum_{y \in X_j} y\right) = \delta_{ij}\mathbb{X}_i,$$

所以 $\mathfrak{S}$(对于 Hadamard 乘法) 也是 $\mathbb{C}[X]^*$ 的一个子代数.

$\mathfrak{S}$ 的结合方案 $\mathfrak{X}(\mathfrak{S})$ 之邻接代数 $\mathfrak{A}=\langle A_0, A_1, \cdots, A_d\rangle$. 注意到 $\mathfrak{X}(\mathfrak{S})$ 的结合关系 $R_i=\{(x, y)|yx^{-1}\in X_i\}=\bigcup\limits_{x_\alpha\in X_i}\underline{R}_\alpha$, 可知 R_i 的邻接矩阵为 $A_i=\sum_{x_\alpha\in X_i}\underline{A}_\alpha$, 因而 $\mathfrak{S}$ 为 $\underline{\mathfrak{A}}$ 的一个子代数, 记 $f=\underline{f}_{|\mathfrak{A}}$, 那么 $f(A_i)=\mathbb{X}_i$, 并且在 f 之下 $\mathfrak{A}$ 同构于 $\mathfrak{S}$. 设 $\mathfrak{A}$ 的本原幂等元为 $E_0, E_1, \cdots, E_d$. 那么 $f(E_0), f(E_1), \cdots, f(E_d)$ 为 $\mathfrak{S}$ 的本原幂等元. 注意到 $\mathbb{C}[X]$ 中的幂等元必为若干个 e_i 之和, 因此存在 $\{0, 1, \cdots, n-1\}$ 的一个分划 $S_0, S_1, \cdots, S_d$ 使得

$$f(E_i)=e_{S_i}=\sum_{\alpha\in S_i}e_\alpha,$$

$e_{S_0}, e_{S_1}, \cdots, e_{S_d}$ 为 $\mathfrak{S}$ 的本原幂等元. 注意到 $E_0=\frac{1}{n}\sum_{i=0}^d A_i$, 可知 $S_0=\{0\}$, 即 $e_{S_0}=e_0$. 进一步我们有

$$\mathbb{X}_i=\sum_{j=0}^d p_i(j)e_{S_j},$$

$$e_{S_i}=\frac{1}{n}\sum_{j=0}^d q_i(j)\mathbb{X}_j,$$

这里 $P=(p_i(j))$ 和 $Q=(q_i(j))$ 分别是 $\mathfrak{X}(\mathfrak{S})$ 的第一和第二特征值矩阵, 并且

$$(ne_{S_i})\circ(ne_{S_j})=\sum_{k=0}^d q_{ij}^k(ne_{S_k}),$$

这里 q_{ij}^k 为 $\mathfrak{X}(\mathfrak{S})$ 的 Krein 参数.

现在考虑 X 的特征标群, 并导出其上对应于 $\mathfrak{S}$ 的 S 环. 因为 X 是有限交换群, 所以 X 的每个不可约表示都是 1 级的, 因而和它的不可约特征标一致. 令 Y 为 X 的全体不可约特征标的集合. 对于 $\chi_1, \chi_2\in Y$, 如下定义乘积 $\chi_1\chi_2$:

$$\chi_1\chi_2(x)=\chi_1(x)\chi_2(x), \quad \forall\, x\in X,$$

那么 $\chi_1\chi_2$ 也是 X 的一个不可约特征标, 因此, Y 作成一个交换群. 熟知 Y 与 X 同构. Y 叫做 X 的*特征标群*. 我们断言: $\underline{\mathfrak{X}}$ 的第一特征值矩阵 $\underline{P}$ 恰为 X 的特征标表. 实际上, 对于 $i\in\{0, 1, \cdots, n-1\}$, 令

$$\Delta_i: x_\alpha\longrightarrow \underline{p}_\alpha(i)\quad \forall\, x_\alpha\in X. \tag{1.21}$$

由 (1.16) 知, Δ_i 是 $\mathbb{C}[X]$ 的一个线性表示, 自然有 $\Delta_i(x_\alpha x_\beta)=\Delta_i(x_\alpha)\Delta_i(x_\beta)$, 因而 $\Delta_i\in Y$. 由于 $\underline{P}$ 满秩, 所以

$$Y=\{\Delta_0, \Delta_1, \cdots, \Delta_{n-1}\}.$$

对于 $i \in \{0, 1, \cdots, n-1\}$, 定义 $\mathbb{C}[X]$ 到 $\mathbb{C}$ 的线性映射

$$\Delta_i^* : x_\alpha \longrightarrow \underline{q}_i(\alpha) \ \ \forall\, x_\alpha \in X.$$

那么, 由于 $\underline{k_i} = \underline{m_i} = 1$, $\underline{q}_i(\alpha) = \overline{\underline{p}\,\alpha(i)} = \Delta_i(x_\alpha)^{-1}$. 因而 $\Delta_i^* = \Delta_i^{-1}$($Y$ 中 Δ_i 的逆元). 显然 $\Delta_0^* = \Delta_0 = \mathbf{1}$($X$ 的单位特征标).

现在来计算 $\Delta_i^*\Delta_j^*$. 对于任 $x_\alpha \in X$, 有

$$\Delta_i^*\Delta_j^*(x_\alpha) = \Delta_i^*(x_\alpha)\Delta_j^*(x_\alpha) = \underline{q}_i(\alpha)\underline{q}_j(\alpha),$$

考虑 (1.19) 两端的 (α, j) 元素, 有

$$\sum_{k=0}^{n-1} \underline{q}_{ij}^k \underline{q}_k(\alpha) = \underline{q}_i(\alpha)\underline{q}_j(\alpha).$$

所以有

$$\Delta_i^*\Delta_j^* = \sum_{k=0}^{n-1} \underline{q}_{ij}^k \Delta_k^*. \tag{1.22}$$

令 $\mathbb{C}[Y]$ 表示 Y 的群环. 那么由 (1.20′) 和 (1.22) 知线性映射

$$\begin{aligned} \varphi : \mathbb{C}[X]^* &\longrightarrow \mathbb{C}[Y] \\ ne_i &\longmapsto \Delta_i^* \end{aligned}$$

给出 $\mathbb{C}[X]^*$ 到 $\mathbb{C}[Y]$ 的一个同构. 在此同构下

$$\varphi : ne_{S_i} \longrightarrow \mathbb{Y}_i = \sum_{\alpha \in S_i} \Delta_\alpha^*,$$

并且有

$$\mathbb{Y}_i\mathbb{Y}_j = \sum_{k=0}^{d} q_{ij}^k \mathbb{Y}_k. \tag{1.23}$$

令 $\mathfrak{S}^* = \langle \mathbb{Y}_0, \mathbb{Y}_1, \cdots, \mathbb{Y}_d \rangle$. 我们断言: $\mathfrak{S}^*$ 是 Y 上的一个 S 环. 实际上, 令 $Y_i = \{\Delta_\alpha^* \in Y | \alpha \in S_i\}$. 显然 S 环定义中条件 (i), (ii) 和 (iv) 被满足. 由于 q_{ij}^k 是 $\mathfrak{X}(\mathfrak{S})$ 的 Krein 参数, 由命题 1.13(iii) 知 $q_{ij}^0 = m_i\delta_{i\hat{j}}$, 于是由 (1.23) 和命题 1.13(v) 可知

$$\mathbb{Y}_i\mathbb{Y}_{\hat{i}} = m_i\mathbb{Y}_0 = m_i\mathbf{1}.$$

因此 $Y_i^{-1} = Y_{\hat{i}}$. 所以 S 环定义中条件 (iii) 亦被满足. 于是 $\mathfrak{S}^*$ 是 Y 上的一个 S 环.

这样, $\mathfrak{S}^*$ 确定了 Y 上的一个交换结合方案 $\mathfrak{X}(\mathfrak{S}^*)$, 它的交叉数恰与 X 上的交换结合方案 $\mathfrak{X}(\mathfrak{S})$ 的 Krein 参数一致, 所以二者是形式对偶的. $\mathfrak{S}^*$ 叫做 $\mathfrak{S}$ 的对偶 S 环.

进一步, 我们对 $Y_i = \{\Delta_\alpha^* \in Y | \alpha \in S_i\}$ 给出一种函数刻画. 注意到

$$\begin{aligned}\Delta_\alpha(e_\beta) =& \Delta_\alpha\left(\frac{1}{n}\sum_{i=0}^{n-1} \underline{q}_\beta(i) x_i\right) \\ =& \frac{1}{n}\sum_{j=0}^{n-1} \underline{q}_\beta(i)\overline{\underline{q}_\alpha(i)} = \delta_{\alpha\beta}.\end{aligned}$$

于是

$$\Delta_\alpha(e_{S_i}) = \begin{cases} 1, & \text{如果 } \alpha \in S_i, \\ 0, & \text{不然}. \end{cases}$$

由于 $e_{S_0}, e_{S_1}, \cdots, e_{S_d}$ 张成 $\mathfrak{S}$, 所以 Δ_α 和 Δ_β 在 $\mathfrak{S}$ 上取值相同, 当且仅当 Δ_α 和 Δ_β 落在同一个 Y_i (注意 $\Delta_\alpha \in Y_i \Longleftrightarrow \Delta_\alpha^* \in Y_{\hat{i}}$).

总结上面的讨论, 我们有

定理 1.14(关于交换群上 S 环的对偶性) 设 $\mathfrak{S}$ 是有限交换群 X 上的一个 S 环, Y 是 X 的特征标群. 设 $\sim$ 是在 Y 上如下定义的等价关系:

$$\Delta_\alpha \sim \Delta_\beta \Longleftrightarrow \Delta_\alpha \text{和} \Delta_\beta \text{在 } \mathfrak{S} \text{ 上的限制重合}.$$

设 $Y_0, Y_1, \cdots, Y_d$ 是全体等价类, 并令 $\mathbb{Y}_i = \sum_{\Delta_\alpha \in Y_i} \Delta_\alpha^*$. 那么 $\mathbb{C}[Y]$ 由 $\mathbb{Y}_0, \mathbb{Y}_1, \cdots, \mathbb{Y}_d$ 生成的子代数 $\mathfrak{S}^*$ 是 Y 上的一个 S 环, 使得 $\dim \mathfrak{S}^* = \dim \mathfrak{S}$, 并且 $\mathfrak{X}(\mathfrak{S}^*)$ 的交叉数恰是 $\mathfrak{X}(\mathfrak{S})$ 的 Krein 参数.

推论 1.15 设 X 是一个有限交换群, 那么对于定理 1.4 中的结合方案 $\mathfrak{X}$, 存在 X 的特征标群 Y 上的结合方案 $\mathfrak{Y}$ 与 $\mathfrak{X}$ 成形式对偶.

最后, 我们讨论 S 环决定的结合方案的特征值. 设 $\mathfrak{S}$ 是有限交换群 X 上的一个 S 环, 生成元为 $\mathbb{X}_0, \mathbb{X}_1, \cdots, \mathbb{X}_d$, 而这些生成元在 X 中对应的类为 $X_0, X_1, \cdots, X_d$. 结合方案 $\mathfrak{X}(\mathfrak{S})$ 的结合类

$$R_i = \{(x, y) \in X \times X | yx^{-1} \in X_i\}, \ i = 0, 1, \cdots, d.$$

设 $|X| = n$. 再设 $Y = \{\Delta_0, \Delta_1, \cdots, \Delta_{n-1}\}$ 是 X 的特征标群, 这里 Δ_i 是由 (1.21) 给出的. 现在将每个特征标 Δ_β 看作 $\mathbb{C}$ 上一个 n 维列向量, 它的第 α 位置上的元素为 $\Delta_\beta(x_\alpha) = \underline{p}_\alpha(\beta)$. 结合方案 $\mathfrak{X}(\mathfrak{S})$ 的结合类 R_i 之邻接矩阵 A_i 有

$$(A_i)_{\alpha\beta} = \begin{cases} 1, & (x_\alpha, x_\beta) \in R_i, \\ 0, & \text{不然}. \end{cases}$$

于是

$$(A_i\Delta_\beta)_\alpha = \sum_{\gamma=0}^{n-1}(A_i)_{\alpha\gamma}\Delta_\beta(x_\gamma) = \sum_{x_\gamma x_\alpha^{-1}\in X_i}\Delta_\beta(x_\gamma)$$
$$= \sum_{x\in X_i}\Delta_\beta(xx_\alpha) = \sum_{x\in X_i}\Delta_\beta(x)\Delta_\beta(x_\alpha),$$

即有

$$A_i\Delta_\beta = \sum_{x\in X_i}\Delta_\beta(x)\cdot\Delta_\beta.$$

令 $\Delta_\beta(\mathbb{X}_i) = \sum_{x\in X_i}\Delta_\beta(x)$, 那么特征标 Δ_β 是 A_i 的属于特征值 $\Delta_\beta(\mathbb{X}_i)$ 的特征向量. 由特征标的第一正交关系知, 不同特征标 Δ_α 和 Δ_β 是正交的, 具体说有

$$\sum_{x\in X}\Delta_\alpha(x)\overline{\Delta_\beta(x)} = |X|\delta_{\alpha\beta}.$$

Δ_α 和 Δ_β 在定理 1.14 中的同一个等价类 Y_j 中, 当且仅当 $\Delta_\alpha(\mathbb{X}_i) = \Delta_\beta(\mathbb{X}_i)$, $i = 0, 1, \cdots, d$. 令 V_j 是由 Y_j 中的特征标 (看作列向量) 张成的子空间, 那么 $V_0\perp\cdots\perp V_d$ 是 $\mathbb{C}^{(n)}$ $(n = |X|)$ 的一个正交直和分解. 这样, 我们有

定理 1.16 结合方案 $\mathfrak{X}(\mathfrak{G})$ 的第一特征值矩阵 P 的 (j, i) 位置元素为

$$p_i(j) = \Delta_\alpha(\mathbb{X}_i),\ i, j = 0, 1, \cdots, d,$$

这里 Δ_α 是等价类 Y_j 中的任一特征标.

§1.6 结合方案的本原性和非本原性

设 $\mathfrak{X} = (X, \{R_i\}_{0\leqslant i\leqslant d})$ 是一个交换结合方案. 令 $\Gamma^{(i)} = (X, R_i)$ 表示以 X 为顶点集而以 R_i 为边集的 (有向) 图, 叫做关系 R_i 的图, 这里 $1\leqslant i\leqslant d$. $\Gamma^{(i)}$ 中从顶点 x 到顶点 y 的一条长为 s 的道路指的是一个顶点序列 $x_0 = x, x_1, \cdots, x_{s-1}, x_s = y$ 使得 $(x_\nu, x_{\nu+1}) \in R_i$, 对于 $\nu = 0, 1, \cdots, s-1$. 图 $\Gamma^{(i)}$ 说是连通的, 如果对于任二不同元素 $x, y\in X$ 在 $\Gamma^{(i)}$ 中存在从 x 到 y 的道路.

结合方案 $\mathfrak{X}$ 叫做本原的, 如果它的关系图 $\Gamma^{(i)}$ $(i = 1, \cdots, d)$ 都是连通的, 否则叫做非本原的.

取定 $\mathfrak{X}$ 的一个关系 R_i 的图 $\Gamma^{(i)}$ $(1\leqslant i\leqslant d)$. 对于 X 的任意一对元素 x 和 y, 考虑邻接矩阵 A_i 的 s 次幂的 (x, y) 元素, 由

$$(A_i^s)_{xy} = \sum_{x_1,\cdots,x_{s-1}}(A_i)_{xx_1}(A_i)_{x_1x_2}\cdots(A_i)_{x_{s-1}y}$$

可知, $(A_i^s)_{xy} \neq 0$ 当且仅当 $\Gamma^{(i)}$ 中存在从 x 到 y 的长为 s 的道路. 另一方面 A_i^s 可表成 $A_0, A_1, \cdots, A_d$ 的线性组合, 并且这种表示是唯一的, 设

$$A_i^s = a_0A_0 + a_1A_1 + \cdots + a_dA_d.$$

如果 $(x, y) \in R_j$ 有 $(A_i^s)_{xy} = a_j \neq 0$, 那么每个 $(x', y') \in R_j$ 均有 $(A_i^s)_{x'y'} \neq 0$.

命题 1.17 对于 $\mathfrak{X}$ 的一个关系图 $\Gamma^{(i)}\,(1 \leqslant i \leqslant d)$, 如下定义 X 上的一个关系 $\sim$:

$$x \sim y \text{ 当且仅当在 } \Gamma^{(i)} \text{ 中存在从 } x \text{ 到 } y \text{ 的道路}.$$

那么 $\sim$ 是一个等价关系, 并且它是某些结合关系 R_j 的并.

证明 上面的分析已经证明了 $\sim$ 是某些 R_j 的并. 现在证明 $\sim$ 是一个等价关系. $\sim$ 的传递性显然成立.

$\sim$ 的反身性: 从 $\Gamma^{(i)}$ 的每个顶点出发都有边 (因为 $k_i \geqslant 1$), 而顶点数 $|X|$ 是有限的, 所以 $\Gamma^{(i)}$ 中存在圈, 即序列 $x_0 = x, x_1, \cdots, x_{s-1}, x_s = x(s \geqslant 2)$ 使得 $(x_\nu, x_{\nu+1}) \in R_i\,(\nu = 0, 1, \cdots, s-1)$. 这就意味着 A_0 在 A_i^s 关于基 $A_0, A_1, \cdots, A_d$ 的线性组合中出现. 于是 $\sim$ 包含关系 R_0. 因此, 对于任 $x \in X$ 均有 $x \sim x$.

最后看 $\sim$ 的对称性, 即 $x \sim y \rightarrow y \sim x$. 由反身性知, A_0 在某个 A_i^s 关于 $A_0, A_1, \cdots, A_d$ 的线性表示式中出现. 考虑 $A_i^s = A_iA_i^{s-1}$, 而 $p_{ij}^0 = k_i\delta_{ij'}$, 所以 A_i^{s-1} 的线性表示式必含 $A_{i'}$, 于是 $\sim$ 包含关系 $R_{i'}$, 这就是说, 如果 $(x, x_1) \in R_i$, 那么 $(x_1, x) \in R_{i'}$, 因而 $x_1 \sim x$. 由此即可推出, 如果 $x \sim y$ 就有 $y \sim x$.

这样证明了 $\sim$ 是 X 上的一个等价关系. 适当重排 $R_1, \cdots, R_d$ 的顺序, 存在一个 $s\,(1 \leqslant s \leqslant d)$ 使得等价关系 $\sim$ 恰为 $R_0, R_1, \cdots, R_s$ 的并 $\bigcup\limits_{j=0}^{s} R_j$. □

X 关于等价关系 $\sim$ 的那些等价类就是 $\Gamma^{(i)}$ 的连通分支. 显然, $\Gamma^{(i)}$ 连通, 当且仅当由 $\Gamma^{(i)}$ 决定的等价关系 $\sim$ 就是全体 R_j 的并.

现在, 我们考虑由群作用确定的结合方案什么时候是本原的? 设 G 是一个有限群, 可迁地作用在有限集 Ω 上. 说 G 是非本原的, 如果存在 Ω 的子集 S 使得 $1 < |S| < |\Omega|$, 并且对于每个 $\sigma \in G$ 均有

$$S^\sigma = S \text{ 或者 } S^\sigma \cap S = \varnothing,$$

这里 $S^\sigma = \{\alpha^\sigma | \alpha \in S\}$. 这样的 S 叫做一个非平凡块(block). $\{S^\sigma | \sigma \in G\}$ 给出 Ω 的一个分划, 叫做 G 的非本原系. 如果不存在非平凡块, 则说 G 是本原的.

定理 1.18 设有限群 G 可迁地作用在集合 Ω 上. 那么 (G, Ω) 确定的结合方案 $\mathfrak{X} = (\Omega, \{\Lambda_i\}_{0 \leqslant i \leqslant d})$ 是本原的当且仅当 G 是本原的.

证明 设 G 不是本原的, 并设 S 是一个非平凡块. 任取 S 的两个不同的元素 x 和 y, 设 $(x, y) \in \Lambda_i$. 我们断言: 关系 Λ_i 的图 $\Gamma^{(i)}$ 不是连通的, 因而 $\mathfrak{X}$ 不是本原

的. 假设 $\Gamma^{(i)}$ 是连通的, 任取一个元素 $z \in \Omega \backslash S$, 那么 $\Gamma^{(i)}$ 中存在从 x 到 z 的道路 $x_0 = x, x_1, \cdots, x_{s-1}, x_s = z$ 使得 $(x_\nu, x_{\nu+1}) \in \Lambda_i$. 注意到 $x_0 \in S$ 而 $x_s \notin S$, 所以存在 j 使得 $x_0, \cdots, x_{j-1} \in S$ 而 $x_j \notin S$. 由于 $(x, y) \in \Lambda_i$, $(x_{j-1}, x_j) \in \Lambda_i$, 而 Λ_i 为一个 G 轨道, 存在 $\sigma \in G$ 使得 $x^\sigma = x_{j-1} \in S$ 而 $y^\sigma = x_j \notin S$. 但由 $x^\sigma \in S$ 知 $S^\sigma = S$, 应有 $y^\sigma \in S$, 矛盾.

反过来. 设 $\mathfrak{X}$ 不是本原的, 那么有某个关系图不连通. 设 $\Gamma^{(i)}$ 不连通, 再设 S 是 $\Gamma^{(i)}$ 的一个连通分支, 那么 $1 < |S| < |\Omega|$. 由于 Λ_i 是一个 G 轨道, 如果 $\Gamma^{(i)}$ 中存在从 x 到 y 的一条道路, 那么对于任意 $\sigma \in G$, $\Gamma^{(i)}$ 中也存在从 x^σ 到 y^σ 的一条道路, 于是 S^σ 也是 $\Gamma^{(i)}$ 的一个连通分支, 因而 $S^\sigma = S$ 或者 $S^\sigma \cap S = \varnothing$, 于是 G 是非本原的. □

这里我们给出 G 是本原群的一个充分必要条件. 我们有

定理 1.19 设有限群 G 可迁地作用在有限集 Ω 上, 任取 $x \in \Omega$. 那么 G 是本原的当且仅当 x 的稳定子 G_x 是 G 的一个极大子群.

证明 设 G 是非本原的, S 是含 x 的一个非平凡块. 令 $K = \{\sigma \in G | S^\sigma = S\}$. 显然, K 是 G 的一个子群, 由于 G 可迁且 $S \neq \Omega$ 知 $K \neq G$. 又由于 $|S| > 1$, 存在 $y \in S$ 但 $y \neq x$. 因 G 是可迁的, 存在 $\sigma \in G$ 使得 $x^\sigma = y$. 那么 $S^\sigma = S$, 因而 $\sigma \in K$. 但 $\sigma \notin G_x$, 所以 $K \neq G_x$. 又显然有 $G_x \subseteq K$, 因而 $G_x \subsetneq K \subsetneq G$, 即 G_x 不是 G 的极大子群.

反过来, 设 G_x 不是 G 的极大子群. 令 K 是 G 的一个子群使得 $G_x \subsetneq K \subsetneq G$. 再令 $S = \{x^\sigma | \sigma \in K\}$. 往证 S 是一个非平凡块. 显然有

$$|\Omega| = |G : G_x| > |K : G_x| \text{ 及 } |S| = |K : G_x| > 1.$$

对于 $\tau \in G$, 设有 $y \in S \cap S^\tau$. 那么存在 $\sigma_1, \sigma_2 \in K$ 使得 $y = x^{\sigma_1} = x^{\sigma_2 \tau}$, 于是 $\sigma_2 \tau \sigma_1^{-1} \in G_x$, $\tau \in \sigma_2^{-1} G_x \sigma_1 \subset K$, 因此 $S^\tau = S$. 这就证明了 S 是一个非平凡块, 因而 G 不是本原的. □

下面我们给出 $\mathfrak{X}$ 是非本原结合方案的几个等价条件.

定理 1.20 设 $\mathfrak{X} = (X, \{R_i\}_{0 \leqslant i \leqslant d})$ 是一个类数为 d 的交换结合方案, A_0, $A_1, \cdots, A_d$ 是 $\mathfrak{X}$ 的邻接矩阵, $E_0, E_1, \cdots, E_d$ 是邻接代数的本原幂等元. 再设 p_{ij}^k 和 q_{ij}^k 分别是 $\mathfrak{X}$ 的交叉数和 Krein 参数. 那么下面的条件等价:

(i) $\mathfrak{X}$ 是非本原的.

(ii) 适当排列 X 中元素的顺序, 存在某个 $i \neq 0$ 使得 A_i 具有形状

$$A_i = \left(\begin{array}{c|c} * & * \\ \hline 0 & * \end{array}\right).$$

(iii) 适当重排指标 $1, 2, \cdots, d$ 的顺序, 存在一个 $s\,(0 < s < d)$ 使得 $A_i A_j$ 是

$A_0, A_1, \cdots, A_s$ 的线性组合, 对于 $0 \leqslant i, j \leqslant s$. 等价地说

$$p_{ij}^k = 0,\ 0 \leqslant i, j \leqslant s,\ s < k.$$

(iv) 适当重排指标 $1, 2, \cdots, d$ 的顺序, 存在一个 $t\,(0 < t < d)$ 使得 $E_i \circ E_j$ 是 $E_0, E_1, \cdots, E_t$ 的线性组合, 对于 $0 \leqslant i, j \leqslant t$. 等价地说

$$q_{ij}^k = 0,\ 0 \leqslant i, j \leqslant t,\ t < k.$$

(v) 存在 $E_i\,(i \neq 0)$, 对于某二元素 $x, y(x \neq y)$ 有 E_i 的第 x 行和第 y 行相同.

证明 设 $\mathfrak{X}$ 是非本原的, 那么某个 $\Gamma^{(i)}\,(i \neq 0)$ 不是连通的. 由命题 1.17 知, 适当重排指标 $1, 2, \cdots, d$ 的顺序, 存在一个 $s\,(0 < s < d)$ 使得 $\bigcup\limits_{\nu=0}^{s} R_\nu$ 是 X 上的一个等价关系, 并且对于 $0 \leqslant \nu \leqslant s$ 有 $0 \leqslant \nu' \leqslant s$. 设 S 是一个等价类, 对于任意 $x \in S$, 注意到 $\sum_{\nu=0}^{s} A_\nu$ 的第 x 行有 $p = \sum_{\nu=0}^{s} k_\nu$ 个 1, 即 S 中有 p 个元素 $x_1, x_2, \cdots, x_p$ 使得 $x_1 \sim x_i$. 由于 S 中任二点 x_i, x_j 均有 $x_i \sim x_j$, 因此 $S = \{x_1, \cdots, x_p\}$, 于是 $\sum_{\nu=0}^{s} A_i$ 中对应于 S 的主子矩阵为 J_p. 每个等价类中的元素个数均为 p, 等价类的个数为 $q = |X|/p$, 适当重排 X 中元素的顺序 (按等价类分组) 就有

$$\sum_{\nu=0}^{s} A_\nu = [\underbrace{J_p, J_p, \cdots, J_p}_{q}] = I_q \otimes J_p, \tag{1.24}$$

这里 J_p 为 p 阶全 1 矩阵, I_q 表示 q 阶单位矩阵, $\otimes$ 表示 Kronecker 积. 令

$$M = \sum_{\nu=0}^{s} A_\nu. \tag{1.25}$$

由 (1.24) 我们有

$$M^2 = pM,\ M \circ M = M,\ M \neq I, M \neq J. \tag{1.26}$$

由 (1.26) 中第一个等式知 $\frac{1}{p}M$ 是 $\mathfrak{X}$ 的邻接代数 $\mathfrak{A}$ 中的一个幂等元, 于是它是 $E_0, E_1, \cdots, E_d$ 的线性组合, 其系数为 0 或 1. 这样适当重排 $E_1, \cdots, E_d$ 的顺序, 可设

$$M = p\sum_{\nu=0}^{t} E_\nu\ (0 < t < d). \tag{1.27}$$

E_0 必须出现在上式中, 这是因为从 (1.25) 知 $\tau(M) = |X|\sum_{\nu=0}^{s} k_\nu \neq 0$, 而 $\tau(E_\nu) = 0$ 对 $\nu \neq 0$.

第一步. 证明 (i)$\Leftrightarrow$(ii). 设 (i) 成立, 由 (1.24) 可知 (ii) 成立. 反之, 设 (ii) 成立, 那么, 有非空子集 S 使得 $x, y \in S$, 对于任意 $l \geqslant 1$ 均有 $(A_i^l)_{xy} = 0$, 即 $\Gamma^{(i)}$ 中没有从 x 到 y 的道路, 所以 $\Gamma^{(i)}$ 不连通.

第二步. 证明 (i)⇔(iii). 设 (i) 成立, 由 (1.25) 有

$$M^2 = \sum_{k=0}^{d} \left(\sum_{i,j=0}^{s} p_{ij}^k \right) A_k.$$

再由 (1.26) 中第一个等式可知, $k > s$ 时 A_k 的系数 $\sum_{i,j=0}^{s} p_{ij}^k = 0$. 因为 p_{ij}^k 为非负的, 所以对于 $0 \leqslant i, j \leqslant s$ 及 $s < k$ 有 $p_{ij}^k = 0$. 因而 (iii) 成立.

反之, 设 (iii) 成立. 显然, 对于 $i\,(0 < i \leqslant s)$ 及任意 $l \geqslant 1$, A_i^l 为 $A_0, A_1, \cdots, A_s$ 的线性组合. 因此, 对于 $(x, y) \in R_k$, $k > s$, 恒有 $(A_i^l)_{xy} = 0$. 就是说 $\Gamma^{(i)}$ 中没有从 x 到 y 的道路, 即 $\Gamma^{(i)}$ 不连通, 即 (i) 成立.

第三步. 证明 (i)⇔(iv). 设 (i) 成立. 由 (1.27) 有

$$\frac{1}{p} M = \sum_{\nu=0}^{t} E_\nu \ (0 < t < d).$$

利用 $E_i \circ E_j = \frac{1}{|X|} \sum_{k=0}^{d} q_{ij}^k E_k$, 从上式可得

$$\left(\frac{1}{p} M\right) \circ \left(\frac{1}{p} M\right) = \frac{1}{|X|} \sum_{k=0}^{d} \left(\sum_{i,j=0}^{t} q_{ij}^k \right) E_k,$$

从 (1.26) 中第二个等式知 $(\frac{1}{p}M) \circ (\frac{1}{p}M) = \frac{1}{p^2} M$. 所以当 $k > t$ 时 $\sum_{ij}^{t} q_{ij}^k = 0$. 由于 Krein 参数 $q_{ij}^k \geqslant 0$, 所以 $q_{ij}^k = 0$, 对于 $0 \leqslant i, j \leqslant t$, $t < k$, 因而 (iv) 成立.

反之, 设 (iv) 成立. 我们来证明 (iii) 成立. 我们断言

$$0 \leqslant \widehat{i} \leqslant t, \ 对每个\ i (0 \leqslant i \leqslant t). \tag{1.28}$$

考虑 E_i 的表示式

$$E_i = \frac{1}{|X|} \sum_{\nu=0}^{d} q_i(\nu) A_\nu.$$

令 $\lambda_0, \lambda_1, \cdots, \lambda_r$ 是 $\{q_i(\nu) | \nu = 0, 1, \cdots, d\}$ 中全体不同的非零数, 令

$$\Phi_l = \sum_{q_i(\nu) = \lambda_l} A_\nu, \ l = 0, 1, \cdots, r.$$

于是

$$E_i = \frac{1}{|X|} \sum_{l=0}^{r} \lambda_l \Phi_l.$$

再令 $E_i^h = \underbrace{E_i \circ \cdots \circ E_i}_{h}$, 那么

$$E_i^h = \frac{1}{|X|^h} \sum_{l=0}^{r} \lambda_l^h \Phi_l, \ h = 0, 1, \cdots, r.$$

因为 $\det(\lambda_l^h)_{0\leqslant l,h\leqslant r} \neq 0$, Φ_l 可表成 $E_0, E_i, E_i^2, \cdots, E_i^r$ 的线性组合 $(0 \leqslant l \leqslant r)$. 因为 E_i^h 是 $E_0, E_1, \cdots, E_t$ 的线性组合 (由假设条件 (iv)), 于是 $\Phi_l\,(0 \leqslant l \leqslant r)$ 亦是 $E_0, E_1, \cdots, E_t$ 的线性组合. 现在

$$E_{\widehat{i}} = {}^tE_i = \overline{E}_i = \frac{1}{|X|}\sum_{l=0}^{r}\overline{\lambda}_l\Phi_l.$$

因此 $E_{\widehat{i}}$ 是 $E_0, E_1, \cdots, E_t$ 的线性组合. 又因 $E_{\widehat{i}}$ 是本原幂等元, 所以对于某个 $j\,(0 \leqslant j \leqslant t)$ 有 $E_{\widehat{i}} = E_j$. 这就证明了 (1.28).

进一步, 由命题 1.13(vi) 及 (1.28), $q_{ij}^k = \frac{m_j}{m_k} q_{\widehat{i}k}^j$, $0 \leqslant \widehat{i} \leqslant t$, 于是

$$q_{ij}^k = 0,\ 0 \leqslant i, k \leqslant t,\ t < j.$$

这样, 我们有

$$\begin{aligned}\left(\sum_{\nu=0}^{t}E_\nu\right)\circ\left(\sum_{\nu=0}^{t}E_\nu\right) &= \frac{1}{|X|}\sum_{k=0}^{d}\left(\sum_{i,j=0}^{t}q_{ij}^k\right)E_k\\ &= \frac{1}{|X|}\sum_{k=0}^{t}\left(\sum_{i=0}^{t}\left(\sum_{j=0}^{d}q_{ij}^k\right)\right)E_k\\ &= \frac{1}{|X|}\left(\sum_{i=0}^{t}m_i\right)\sum_{k=0}^{t}E_k.\end{aligned}$$

令 $p = |X|/\sum_{i=0}^{t}m_i$, $M = p\sum_{\nu=0}^{t}E_\nu$. 由上式有 $M \circ M = M$, 即 M 为 $\widehat{\mathfrak{A}}$ 中的一个幂等元, 所以 M 为 $A_0, A_1, \cdots, A_d$ 的线性组合, 系数为 0 或 1. 于是重排一下 $A_1, \cdots, A_d$ 的顺序, 可设

$$M = \sum_{\nu=0}^{s}A_\nu\quad(0 < s < d).$$

注意到 A_0 出现在这个和式中, 因为 $\mathrm{tr}M = p(\sum_{i=0}^{t}m_i) \neq 0$, 而 $\mathrm{tr}A_\nu = 0$ 对于 $\nu \neq 0$. 由于 $M^2 = pM$, 而交叉数 p_{ij}^k 为非负的, 所以 A_iA_j 是 $A_0, A_1, \cdots, A_s$ 的线性组合, 对于 $0 \leqslant i, j \leqslant s$, 这就推出条件 (iii) 成立. (b) 中已证明了 (iii)$\Leftrightarrow$ (i).

第四步. 证明 (i)$\Leftrightarrow$(v). 设 (i) 成立, 于是可设

$$\sum_{\nu=0}^{s}A_\nu = p\sum_{i=0}^{t}E_i = I_q \otimes J_p\ (0 < s < d;\ 0 < t < d),$$

这里 $p = \sum_{\nu=0}^{s}k_\nu$, $q = |X|/p = \sum_{i=0}^{t}m_i$. 于是存在两个不同的元素 x 和 y 使得 $\sum_{i=0}^{t}E_i$ 的第 x 行和第 y 行相同, 即

$$e_x\sum_{i=0}^{t}E_i = e_y\sum_{i=0}^{t}E_i.$$

回忆 1.3 中所述, E_i 为 V 到 V_i 的正投影, 所以 $e_xE_i = e_yE_i\,(0 \leqslant i \leqslant t)$, 即 E_i 的第 x 行和第 y 行相同. 于是 (v) 成立.

反过来设 (v) 成立. 我们在 X 上如下定义一个等价关系 $\sim$:

$$x \sim y \text{ 当且仅当 } E_i \text{ 的第 } x \text{ 行和第 } y \text{ 行相同.}$$

我们证明, 适当重排 $R_1, \cdots, R_d$ 的顺序, 存在 $s\,(0 < s < d)$ 使得这个等价关系恰为 $R_\nu\,(0 \leqslant \nu \leqslant s)$ 的并. 设

$$E_i = \frac{1}{|X|}\sum_{\alpha=0}^{d} q_i(\alpha)A_\alpha,$$

并假定 E_i 的第 x 行和第 y 行相同, 即 $(E_i)_{xz} = (E_i)_{yz}$ 对所有 $z \in X$. 设 $(x,\, y) \in R_\gamma$, 并设 $(x,\, z) \in R_\alpha$, $(y,\, z) \in R_\beta$. 那么有 $(E_i)_{xz} = \frac{1}{|X|}q_i(\alpha)$, $(E_i)_{yz} = \frac{1}{|X|}q_i(\beta)$. 因此

$$q_i(\alpha) = q_i(\beta) \text{ 只要 } p^\gamma_{\alpha\beta'} \neq 0. \tag{1.29}$$

注意到条件 (1.29) 不依赖于 $(x,\, y) \in R_\gamma$ 的选取, 所以 R_γ 包含在这个等价关系 $\sim$ 之中. 适当重排 $R_1, \cdots, R_d$ 的顺序, 就有 $\sim$ 是结合关系 $R_\nu\,(0 \leqslant \nu \leqslant s)$ 之并. 如果 $s = d$, 那么 E_i 的行全相同. 又因 ${}^t\overline{E}_i = E_i$, E_i 的列也相同, 这与 $i \neq 0$ 矛盾. 因此 $s < d$. 又显然 $0 < s$(因假设 E_i 至少有两行相同). 于是可推得 (1.24), 因而 $\mathfrak{X}$ 是非本原的. □

§1.7 非本原结合方案的子方案和商方案

设 $\mathfrak{X} = (X,\, \{R_i\}_{0\leqslant i\leqslant d})$ 是非本原的交换结合方案, 就是说, 定理 1.20 中的 (i)~(v) 任一成立. 设关系 R_α 的图 $\Gamma^{(\alpha)}$ 不连通, 那么适当重排 $R_1, \cdots, R_d$ 的顺序, 存在 $s\,(0 < s < d)$ 使得由 $\Gamma^{(\alpha)}$ 决定的等价关系是 $R_0, \cdots, R_s$ 的并 $\bigcup\limits_{i=0}^{s} R_i$. 关于这个等价关系的等价类叫做块, 它们就是图 $\Gamma^{(\alpha)}$ 的连通分支. 块的大小均为 $p = \sum_{i=0}^{s} k_i$, 块的个数为 $q = |X|/p$. 令 Σ 为这些块的集合, 叫做 $\mathfrak{X}$ 的非本原系.

再适当重排本原幂等元 $E_1, \cdots, E_d$ 的顺序, 可使得存在 $t\,(0 < t < d)$ 有下面的等式

$$M = \sum_{i=0}^{s} A_i = p\sum_{i=0}^{t} E_i = I_q \otimes J_p, \tag{1.30}$$

这里 $q = |X|/p = \sum_{i=0}^{t} m_i$. 这时每个块都对应 (1.30) 中主对角线上的一个 p 阶矩阵 J_p.

设 S 是一个块 $(S \in \Sigma)$. 那么容易看出

$$\mathfrak{X}_S = (S,\, \{R_i\}_{0\leqslant i\leqslant s})$$

是一个交换结合方案, 叫做 $\mathfrak{X}$ 的一个结合子方案(association subscheme), 这里 R_0, $R_1, \cdots, R_s$ 理解为它们在 S 上的限制.

$\mathfrak{X}_S$ 的邻接矩阵是 $A_i\,(i=0,1,\cdots,s)$ 中对应于块 S 的子矩阵. 显然 $\mathfrak{X}_S$ 的交叉数为 $p_{ij}^k\,(i,j,k=0,1,\cdots,s)$. 设 $\mathfrak{X}$ 的邻接代数为 $\mathfrak{A}=\langle A_0, A_1, \cdots, A_d\rangle$. 那么 $\mathfrak{X}_S$ 的邻接代数同构于 $\mathfrak{A}$ 的子代数 $\mathfrak{A}_S=\langle A_0, A_1, \cdots, A_s\rangle$.

对于两个不同的块 S_1 和 S_2, 结合方案 $\mathfrak{X}_{S_1}$ 和 $\mathfrak{X}_{S_2}$ 有相同的交叉数, 但它们不一定同构. 下面我们要在全体块的集合 Σ 上定义一个结合方案, 叫做 $\mathfrak{X}$ 在 Σ 上的商方案.

定理 1.21 设 $\mathfrak{X}=(X,\{R_i\}_{0\leqslant i\leqslant d})$ 是一个非本原的交换结合方案, 有非本原系 Σ, 按 $\mathfrak{X}$ 的块适当重排 A_i 和 E_i 的顺序, 可设

$$M=\sum_{i=0}^{s}A_i=p\sum_{i=0}^{t}E_i=I_q\otimes J_p.$$

在 $\{0,1,\cdots,d\}$ 上如下定义关系 $\sim$:

$$i\sim j \text{ 当且仅当存在 } \alpha(0\leqslant\alpha\leqslant s) \text{ 使 } p_{i\alpha}^j\neq 0.$$

那么

(1) $\sim$ 是一个等价关系.

(2) 设 $T_0, T_1, \cdots, T_r$ 是由 $\sim$ 决定的等价类, 那么 $r=t$.

(3) 设 $D_i=\sum_{\alpha\in T_i}A_\alpha$, 那么存在 q 阶矩阵 $\widetilde{D_i}$ 使得 $D_i=\widetilde{D_i}\otimes J_p$, 并且 $\widetilde{D_i}\,(i=0,1,\cdots,t)$ 是 $\sum$ 上一个结合方案的邻接矩阵. 这个结合方案叫做 $\mathfrak{X}$ 的商结合方案(quotient association scheme), 记作 $\mathfrak{X}(\Sigma)$.

(4) $E_0, E_1, \cdots, E_t$ 是由 $\frac{1}{p}D_0, \frac{1}{p}D_1, \cdots, \frac{1}{p}D_t$ 张成的代数之本原幂等元, 而这个代数同构于 $\mathfrak{X}(\Sigma)$ 的邻接代数.

证明 由命题 1.17 知, 对于 $0\leqslant i\leqslant s$ 恒有 $0\leqslant i'\leqslant s$, 所以 M 是对称矩阵, 即 ${}^tM=M$.

(1) 往证 $\sim$ 是等价关系. 由命题 1.1(ii), $p_{i0}^i=1$, 所以 $i\sim i$. 再由命题 1.1(iv) $k_jp_{i\alpha}^j=k_ip_{j\alpha'}^i$ 可知, 如果 $i\sim j$, 那么 $j\sim i$. 因此 $\sim$ 是自反的和对称的. 再来证明 $\sim$ 是传递的. 设 $i\sim j$ 及 $j\sim k$. 那么存在 $\alpha,\beta(0\leqslant\alpha,\beta\leqslant s)$ 使 $p_{i\alpha}^j\neq 0$ 及 $p_{j\beta}^k\neq 0$. 取 $(w,z)\in R_k$, 存在 $y\in X$ 使 $(w,y)\in R_j$ 和 $(y,z)\in R_\beta$, 又存在 $x\in X$ 使 $(w,x)\in R_i$ 和 $(x,y)\in R_\alpha$. 设 $(x,z)\in R_\gamma$, 那么 $p_{i\gamma}^k\neq 0$. 又由 $(x,y)\in R_\alpha$ 及 $(y,z)\in R_\beta$, 可知 $(A_\alpha A_\beta)_{xz}\neq 0$. 而 $A_\alpha A_\beta$ 可表成 $A_0, A_1, \cdots, A_s$ 的线性组合, 所以可知 $0\leqslant\gamma\leqslant s$. 于是就有 $i\sim k$.

(2) 设 $T_0, T_1, \cdots, T_r$ 是 $\{0,1,\cdots,d\}$ 在等价关系 $\sim$ 之下的全体等价类, T_0 是包含 0 的那个等价类. 那么

$$T_0=\{0,1,\cdots,s\}.$$

这是因为 $i \sim 0$ 当且仅当 $p_{i\alpha}^0 \neq 0$ 对某个 $\alpha \in \{0, 1, \cdots, s\}$, 而 $p_{i\alpha}^0 = k_i\delta_{i\alpha'} \neq 0$, 当且仅当 $i = \alpha' \in \{0, 1, \cdots, s\}$.

又因为 $p_{i\alpha}^j = p_{i'\alpha'}^{j'}$, 所以 $i \sim j$ 当且仅当 $i' \sim j'$. 于是 $T_i' = \{\beta' | \beta \in T_i\}$ 也是一个等价类, 因而存在 $\bar{i}\,(0 \leqslant \bar{i} \leqslant r)$ 使得

$$T_i' = T_{\bar{i}}.$$

我们进一步证明, 对于任给的块 S_1 和 S_2 均有

$$\{\alpha | R_\alpha \cap (S_1 \times S_2) \neq \varnothing\} = T_i, \quad \text{对某个}\, i. \tag{1.31}$$

设 $R_\alpha \cap (S_1 \times S_2) \neq \varnothing$, 我们证明 $R_\beta \cap (S_1 \times S_2) \neq \varnothing$ 当且仅当 $\beta \sim \alpha$. 设 $(x_0, y_0) \in R_\alpha \cap (S_1 \times S_2)$, $(x_1, y_1) \in R_\beta \cap (S_1 \times S_2)$. 又设 $(x_0, y_1) \in R_\gamma$, $(x_0, x_1) \in R_\mu$, 那么 $p_{\beta\mu}^\gamma = p_{\mu\beta}^\gamma \neq 0$. 因为 $x_0, x_1 \in S_1$, 所以 $0 \leqslant \mu \leqslant s$. 于是 $\beta \sim \gamma$. 又设 $(y_1, y_0) \in R_\nu$, 那么 $p_{\gamma\nu}^\alpha \neq 0$, 且 $0 \leqslant \nu \leqslant s$ (因 $y_0, y_1 \in S_2$). 所以 $\gamma \sim \alpha$. 因此 $\beta \sim \alpha$.

反之, 设 $\beta \sim \alpha$, 即存在 $0 \leqslant \lambda \leqslant s$ 使 $p_{\beta\lambda}^\alpha \neq 0$. 注意到 $(x_0, y_0) \in R_\alpha$, 于是存在 $y \in X$ 使 $(x_0, y) \in R_\beta$ 及 $(y, y_0) \in R_\lambda$. 因为 $0 \leqslant \lambda \leqslant s$ 而 $y_0 \in S_2$, 所以 $y \in S_2$. 这样 $(x_0, y) \in R_\beta \cap (S_1 \times S_2)$. 这就证明了 (1.31) 成立.

(3) 令

$$D_i = \sum_{\alpha \in T_i} A_\alpha, \quad i = 0, 1, \cdots, r.$$

由 (1.31) 知, 对于任意两个块 S_1 和 S_2, D_i 的 $S_1 \times S_2$ 子矩阵或为 0 或者为 J_p, 于是

$$D_i = \widetilde{D}_i \otimes J_p, \quad i = 0, 1, \cdots, r, \tag{1.32}$$

这里 $\widetilde{D}_i$ 为 q 阶 (0,1) 矩阵. 易见 $\widetilde{D}_i\,(i = 0, 1, \cdots, r)$ 满足

$$\widetilde{D}_0 = I_q, \quad \widetilde{D}_0 + \widetilde{D}_1 + \cdots + \widetilde{D}_r = J_q, \quad {}^t\widetilde{D}_i = \widetilde{D}_{\bar{i}}.$$

由 (1.32) 可知,

$$D_i D_j = p\widetilde{D}_i\widetilde{D}_j \otimes J_p. \tag{1.33}$$

因此, 对于任意两个块 S_1 和 S_2, D_iD_j 的 $S_1 \times S_2$ 子矩阵为 J_p 的倍数. 另一方面,

$$D_i D_j = \sum_{\gamma=0}^{d} \left(\sum_{\alpha \in T_i} \sum_{\beta \in T_j} p_{\alpha\beta}^\gamma \right) A_\gamma,$$

于是可知, 如果 $\mu \sim \nu$, 那么 A_μ 和 A_ν 的系数相同. 因此有

$$D_i D_j = \sum_{k=0}^{r} \left(\sum_{\alpha \in T_i} \sum_{\beta \in T_j} p_{\alpha\beta}^\gamma \right) D_k, \quad \gamma \in T_k. \tag{1.34}$$

记 $\widetilde{p}_{ij}^k = \frac{1}{p}\sum_{\alpha\in T_i}\sum_{\beta\in T_j} p_{\alpha\beta}^{\gamma}$, $\gamma \in T_k$. 那么由 (1.33) 和 (1.34) 有

$$\widetilde{D}_i\widetilde{D}_j = \sum_{k=0}^{r} \widetilde{p}_{ij}^k \widetilde{D}_k. \tag{1.35}$$

又显然有 $\widetilde{p}_{ij}^k = \widetilde{p}_{ji}^k$. 注意到 $\sum_{i=0}^{r}\widetilde{D}_i = J_q$, 可知 $\widetilde{p}_{ij}^k$ 为非负整数. 于是 $\widetilde{D}_i\,(i = 0, 1, \cdots, r)$ 满足 1.1 中的条件 (i)′~(v)′. 因此, 它们确定 Σ 上的一个交换结合方案, 即 $\mathfrak{X}$ 在 Σ 上的商方案 $\mathfrak{X}(\Sigma)$.

(4) 由 (1.30) 可知, 对于同一块 S 中的 x 和 x_1, M 的第 x 行和第 x_1 行相同, 而 $M = p\sum_{i=0}^{t} E_i$, E_i 为 $\mathbb{C}^{|X|}$ 到 V_i 的正投影, 所以 E_i 的第 x 行和第 x_1 行相同. 又 ${}^tM = M$, $E_i = {}^tE_{\widehat{i}}\,(0 \leqslant i, \widehat{i} \leqslant t)$, 因此 E_i 的第 x 列和第 x_1 列也相同. 这样对于任意块 S_1 和 S_2, E_i 的 $S_1 \times S_2$ 子矩阵为 J_p 的倍数. 于是存在 q 阶矩阵 $\widetilde{E_i}$ 使得

$$E_i = \widetilde{E_i} \otimes J_p, \qquad i = 0, 1, \cdots, t.$$

又 $E_i = \frac{1}{|X|}\sum_{\alpha=0}^{d} q_i(\alpha)A_\alpha$, 于是可知, 如果 $\alpha \sim \beta$, 那 A_α 和 A_β 的系数相同, 因此有

$$E_i = \frac{1}{|X|}\sum_{j=0}^{r} q_i(\alpha_j)D_j, \qquad \text{这里 } \alpha_j \in T_j,\ i = 0, 1, \cdots, t. \tag{1.36}$$

令 $\underline{\mathfrak{A}} = \langle \frac{1}{p}D_0, \frac{1}{p}D_1, \cdots, \frac{1}{p}D_r \rangle$, 它是 $\mathfrak{X}$ 的邻接代数 $\mathfrak{A}$ 的一个 $r+1$ 维子代数. 再令 $\widetilde{\mathfrak{A}}$ 为 $M_q(\mathbb{C})$ 中由 $\widetilde{D}_0, \widetilde{D}_1, \cdots, \widetilde{D}_r$ 张成的子代数, 即 $\mathfrak{X}(\Sigma)$ 的邻接代数. 那么由 (1.34) 和 (1.35) 可知线性映射

$$\begin{aligned} f : \underline{\mathfrak{A}} &\longrightarrow \widetilde{\mathfrak{A}} \\ \tfrac{1}{p}D_i &\longmapsto \widetilde{D}_i \end{aligned}$$

是一个代数同构. 由 (1.36) 知 $E_i\,(0 \leqslant i \leqslant t)$ 是 $\underline{\mathfrak{A}}$ 的本原幂等元, 并且 $\underline{\mathfrak{A}}$ 的单位元

$$\frac{1}{p}D_0 = \frac{1}{p}\sum_{i=0}^{s} A_i = \frac{1}{p}I_q \otimes J_p = \sum_{i=0}^{t} E_i.$$

所以 $E_i (0 \leqslant i \leqslant t)$ 是 $\underline{\mathfrak{A}}$ 的全部本原幂等元, 并且 $r = t$. □

进一步, 我们可以算出商方案 $\mathfrak{X}(\Sigma)$ 的特征值. 记 $\widetilde{E_i} = f(E_i)$. 由 (1.36) 有

$$\widetilde{E_i} = \frac{1}{q}\sum_{j=0}^{t} q_i(\alpha_j)\widetilde{D_j},\ \alpha_j \in T_j,\ i = 0, 1, \cdots, t.$$

于是 $\mathfrak{X}(\Sigma)$ 的第二特征矩阵 $\widetilde{Q} = (\widetilde{q}_i(j))$, 这里 $\widetilde{q}_i(j) = q_i(\alpha_j)$, $\alpha_j \in T_j$. 注意到 $E_j\,(j = 0, 1, \cdots, t)$ 为 $\underline{\mathfrak{A}}$ 的基. 所以

$$\frac{1}{p}D_i = \frac{1}{p}\sum_{\alpha\in T_i} A_\alpha = \sum_{j=0}^{t}\left(\frac{1}{p}\sum_{\alpha\in T_i} p_\alpha(j)\right)E_j.$$

因而有

$$\widetilde{D}_i = \sum_{j=0}^{t}\left(\frac{1}{p}\sum_{\alpha\in T_i} p_\alpha(j)\right)\widetilde{E}_j.$$

于是 $\mathfrak{X}(\Sigma)$ 的第一特征值矩阵 $\widetilde{P} = (\widetilde{p}_i(j))$, 这里

$$\widetilde{p}_i(j) = \frac{1}{p}\sum_{\alpha\in T_i} p_\alpha(j).$$

定理 1.22 设有限群 G 可迁地作用在有限集 Ω 上, 并设 (G, Ω) 确定的结合方案 $\mathfrak{X} = (\Omega, \{\Lambda_i\}_{0\leqslant i\leqslant d})$ 是交换的. 如果 $\mathfrak{X}$ 不是本原的, 而 Σ 是它的非本原系, 那么 $\mathfrak{X}$ 在 Σ 上的商方案和 (G, Σ) 确定的结合方案是一致的.

证明 设非本原系 Σ 是 Ω 关于等价关系 $\bigcup\limits_{i=0}^{s}\Lambda_i\,(0<s<d)$ 的全体等价类. 令 $T_0, T_1, \cdots, T_t$ 是定理 1.21 中定义的 $\{0, 1, \cdots, d\}$ 的全体等价类. 令

$$R_i = \bigcup_{\alpha\in T_i}\Lambda_\alpha, \qquad i = 0, 1, \cdots, t.$$

由 (1.31) 可知, 存在 $\Sigma\times\Sigma$ 的子集 $\widetilde{\Lambda}_i$ 使得

$$R_i = \bigcup_{(S_1,S_2)\in\widetilde{\Lambda}_i} S_1\times S_2, \qquad i = 0, 1, \cdots, t. \tag{1.37}$$

我们断言: $\widetilde{\Lambda}_i\,(i = 0, 1, \cdots, t)$ 恰为 G 在 $\Sigma\times\Sigma$ 上的轨道. 设 $(S_1, S_2)\in\widetilde{\Lambda}_i$, $\sigma\in G$. 往证 $(S_1, S_2)^\sigma\in\widetilde{\Lambda}_i$. 由于 $(S_1, S_2)\in\widetilde{\Lambda}_i$, 我们有

$$S_1\times S_2 = \bigcup_{\alpha\in T_i}\Lambda_\alpha\cap(S_1\times S_2).$$

任取 $(x, y)\in S_1\times S_2$, 那么存在 $\alpha\in T_i$ 使 $(x, y)\in\Lambda_\alpha$. 因为 Λ_α 为 Ω 的 G 轨道, 所以 $(x^\sigma, y^\sigma)\in\Lambda_\alpha$, 于是 $(x^\sigma, y^\sigma)\in R_i$. 注意到 $(x^\sigma, y^\sigma)\in S_1^\sigma\times S_2^\sigma$ 而 S_1^σ 和 S_2^σ 仍为块, 所以 $(S_1, S_2)^\sigma\in\widetilde{\Lambda}_i$.

另一方面, 设 $(S_1, S_2), (S_1', S_2')\in\widetilde{\Lambda}_i$, 往证存在 $\sigma\in G$ 使 $S_1^\sigma = S_1'$, $S_2^\sigma = S_2'$. 任取 $(x, y)\in S_1\times S_2$, $(x', y')\in S_1'\times S_2'$. 设 $(x, y)\in\Lambda_\alpha$, $(x', y')\in\Lambda_\beta$, $\alpha, \beta\in T_i$. 由 G 在 Ω 上可迁, 存在 $\psi\in G$ 使 $x^\psi = x'$, 于是 $(x', y^\psi)\in\Lambda_\alpha$, $y^\psi\in S_2^\psi$. 因为 $\alpha\sim\beta$, $p_{\alpha\nu}^{\beta}\neq 0$ 对某个 $0\leqslant\nu\leqslant s$, 于是存在 $y''\in S_2'$ 使得 $(x', y'')\in R_\alpha$ 且 $(y'', y')\in R_\nu$. 现在 (x', y^ψ) 和 (x', y'') 均在 Λ_α 中. 于是存在 $\rho\in G$ 使 $x'^\rho = x'$ 而 $y^{\psi\rho} = y''\in S_2'$. 记 $\sigma = \psi\rho$, 就有 $(S_1, S_2)^\sigma = (S_1', S_2')$.

于是定理 1.21 中的邻接矩阵 $\widetilde{D}_i$ 的元素为

$$(\widetilde{D}_i)_{S_1S_2} = \begin{cases} 1, & \text{如果 } (S_1, S_2)\in\widetilde{\Lambda}_i, \\ 0, & \text{如果 } (S_1, S_2)\notin\widetilde{\Lambda}_i. \end{cases}$$

它们恰好是 $\widetilde{\Lambda}_i$ 的邻接矩阵. 因此商方案 $\mathfrak{X}(\Sigma)$ 与 (G, Σ) 确定的结合方案重合. □

§1.8 $P(Q)$ 多项式结合方案

设 $\mathfrak{X}=(X,\{R_i\}_{0\leqslant i\leqslant d})$ 是一个对称结合方案, 即它的每个结合关系 R_i 都是对称的:

$$(x,y)\in R_i \Leftrightarrow (y,x)\in R_i\ (i=0,1,\cdots,d).$$

对称结合方案都是交换的. R_i 的邻接矩阵 A_i 都是对称的, 因此它们的特征值都是实数. 在这一节中, 我们介绍一类特殊的结合方案, 即所谓的 P 多项式方案, 它们是结合方案理论中一个重要部分.

对称结合方案 $\mathfrak{X}=(X,\{R_i\}_{0\leqslant i\leqslant d})$ 称为关于顺序 $R_0,R_1,\cdots,R_d$ 的*P 多项式结合方案*, 如果存在复系数 i 次多项式 $v_i(x)$ 使得 $A_i=v_i(A_1)$, 这里 A_i 是关系 R_i 的邻接矩阵 (后面将证明 $v_i(x)$ 具有有理系数).

我们采用下面的符号: 三对角线矩阵

$$B=\begin{pmatrix} a_0 & c_1 & & & \\ b_0 & a_1 & \ddots & & 0 \\ & b_1 & \ddots & c_{d-1} & \\ 0 & & \ddots & a_{d-1} & c_d \\ & & & b_{d-1} & a_d \end{pmatrix},$$

记作

$$B=\left\{\begin{matrix} * & c_1 & c_2 & \cdots & c_{d-1} & c_d \\ a_0 & a_1 & a_2 & \cdots & a_{d-1} & a_d \\ b_0 & b_1 & b_2 & \cdots & b_{d-1} & * \end{matrix}\right\}.$$

定理 1.23 设 $\mathfrak{X}=(X,\{R_i\}_{0\leqslant i\leqslant d})$ 是一个对称结合方案, A_i 是 R_i 的邻接矩阵, $B_1=(p_{1i}^j)$ 为关系 R_1 的交叉矩阵, $P=(p_i(j))$ 是第一特征值矩阵. 那么下面的 (i), (ii), (iii) 彼此等价.

(i) $\mathfrak{X}$ 关于顺序 $R_0,R_1,\cdots,R_d$ 是 P 多项式的, 即存在 i 次多项式 $v_i(x)$ 使得

$$A_i=v_i(A_1),\ i=0,1,\cdots,d.$$

(ii) 存在 i 次多项式 $v_i(x)$ 使得 P 满足

$$p_i(j)=v_i(\theta_j),\ i,j=0,1,\cdots,d,\ \theta_j=p_1(j).$$

(iii) R_1 的交叉矩阵 B_1 为三对角线矩阵, 并且它的对角线旁的元素不为 0, 即

$$B_1=\left\{\begin{matrix} * & 1 & c_2 & \cdots & c_{d-1} & c_d \\ 0 & a_1 & a_2 & \cdots & a_{d-1} & a_d \\ k & b_1 & b_2 & \cdots & b_{d-1} & * \end{matrix}\right\},$$

其中 $b_i \neq 0$, $c_i \neq 0$, k 为 R_1 的价.

证明 (1) 先证 (i)⇔(ii). 设 $E_0, E_1, \cdots, E_d$ 是 $\mathfrak{X}$ 的邻接代数的本原幂等元. 令 $\theta_j = p_1(j)$, 那么有

$$A_1 = \sum_{j=0}^{d} \theta_j E_j.$$

于是对于多项式 $v_i(x)$ 就有

$$v_i(A_1) = \sum_{j=0}^{d} v_i(\theta_j) E_j.$$

设 (i) 成立, 即设 $A_i = v_i(A_1)$, 立得 $p_i(j) = v_i(\theta_j)$, 即 (ii) 成立.

反之, 设 (ii) 成立. 那么有

$$A_i = \sum_{j=0}^{d} p_i(j) E_j = \sum_{j=0}^{d} v_i(\theta_j) E_j = v_i(A_1),$$

即 (i) 成立.

(2) 再证 (i)⇔(iii). 设 (iii) 成立. 由于 $B_1 = (p_{1i}^j)$ 为三对角线的, 有

$$A_1 A_i = b_{i-1} A_{i-1} + a_i A_i + c_{i+1} A_{i+1},$$

这里 $b_{-1} = 0$(约定), $b_0 = k$, $a_0 = 0$, $c_1 = 1$.

令 $v_0(x) = 1$, $v_1(x) = x$, $v_i(x)$ 为如下递归关系定义的 i 次多项式

$$x v_i(x) = b_{i-1} v_{i-1}(x) + a_i v_i(x) + c_{i+1} v_{i+1}(x), 0 \leqslant i \leqslant d-1$$

(注意 $v_i(x)$ 的系数为有理数). 那么有 $A_i = v_i(A_1)$. 因而 (i) 成立.

设 (i) 成立. 因为 $x v_i(x)$ 是 $i+1$ 次多项式, 它可以表成 $v_{i+1}(x), \cdots, v_0(x)$ 的线性组合, 所以 $A_1 A_i$ 是 $A_{i+1}, \cdots, A_1, A_0$ 的线性组合, 其中 A_{i+1} 的系数不为 0, 即 $p_{1i}^{i+1} \neq 0$. 而 $j \geqslant i+2$ 时 $p_{1i}^j = 0$. 因为 $\mathfrak{X}$ 是对称的, 所以有 $p_{1i}^j = 0$ 当且仅当 $p_{1j}^i = 0$. 于是我们有 $p_{1i}^j = 0$, 如果 $|i-j| \geqslant 2$; 且 $p_{1i}^j \neq 0$, 如果 $|i-j| = 1$, 即 (iii) 成立. □

P 多项式结合方案和距离正则图本质上是一回事. 现在我们给出距离正则图的定义. 设 Γ 是一个有限无向图, 它有顶点集 X. 对于 Γ 的两个顶点 x 和 y, 说顶点序列 $x = x_0, x_1, \cdots, x_s = y$ 是 x 和 y 之间的一条长为 s 的道路, 如果 (x_i, x_{i+1}) 都是 Γ 的边 $(i = 0, 1, \cdots, s-1)$. x 与 y 之间最短道路之长叫做 x 与 y 之间的距离, 记作 $\partial(x, y)$. 显然, 下面的三角形不等式成立

$$\partial(x, y) \leqslant \partial(x, z) + \partial(z, y). \tag{1.38}$$

Γ 中两顶点间距离之最大值叫做 Γ 的直径, 记作 $d(\Gamma)$. 令

$$R_i = \{(x, y)|\partial(x, y) = i\}, \ i = 0, 1, \cdots, d.$$

设 x 是 Γ 的一个顶点, 令

$$\Gamma_i(x) = \{y|\partial(x, y) = i\}, i = 0, 1, \cdots, d.$$

特别记 $\Gamma(x) = \Gamma_1(x)$.

图 Γ 叫做距离正则的, 如果 Γ 连通并且 $\mathfrak{X} = (X, \{R_i\}_{0\leqslant i\leqslant d})$ 成为 X 上的一个对称结合方案.

我们有

定理 1.24　设 Γ 是一个连通无向图, 其顶点集为 X. 那么 Γ 是距离正则的, 当且仅当对于任意 i 及距离为 i 的两个顶点 x 和 y,

$$\left.\begin{aligned} c_i &= |\Gamma_{i-1}(x) \cap \Gamma(y)|, & 1 \leqslant i \leqslant d, \\ a_i &= |\Gamma_i(x) \cap \Gamma(y)|, & 0 \leqslant i \leqslant d, \\ b_i &= |\Gamma_{i+1}(x) \cap \Gamma(y)|, & 0 \leqslant i \leqslant d-1 \end{aligned}\right\} \tag{1.39}$$

仅与 i 有关而与顶点 x, y 的选取无关, 其中 d 为 Γ 的直径.

证明　设 Γ 为距离正则图, 那么依定义, $\mathfrak{X} = (X, \{R_i\}_{0\leqslant i\leqslant d})$ 是一个对称结合方案. 因而, 对于 $0 \leqslant i, j, k \leqslant d$ 及 $(x, y) \in R_k$, 常数

$$p_{ij}^k = |\Gamma_i(x) \cap \Gamma_j(y)|$$

仅与 i, j, k 有关, 而与 x, y 的选取无关. 由于 (1.39) 中的 c_i, a_i 及 b_i 分别是

$$c_i = p_{1\,i-1}^i, \ a_i = p_{1\,i}^i, \ b_i = p_{1\,i+1}^i.$$

所以 c_i, a_i, b_i 仅与 i 有关而与 $(x, y) \in R_i$ 的 x, y 无关.

现在反过来, 设 Γ 是一个连通图, 并且 (1.39) 中的 c_i, a_i, b_i 仅与 i 有关, 而与 $\partial(x,y) = i$ 的 x,y 无关. 往证 $\mathfrak{X} = (X, \{R_i\}_{0\leqslant i\leqslant d})$ 是一个对称结合方案, 这里 $R_i = \{(x, y)|\partial(x, y) = i\}$. 由三角形不等式 (1.38) 可知, 对于 $(x, y) \in R_i$, 恒有

$$|\Gamma_j(x) \cap \Gamma(y)| = 0, \text{ 如果 } |i-j| \geqslant 2.$$

再由 Γ 的连通性, 有

$$|\Gamma_j(x) \cap \Gamma(y)| \neq 0, \text{ 如果 } |j-i| = 1. \tag{1.40}$$

令 A_i 为 R_i 的邻接矩阵, 那么由 (1.39) 和 (1.40) 有

$$A_1 A_i = b_{i-1} A_{i-1} + a_i A_i + c_{i+1} A_{i+1}.$$

特别地

$$A_1 A_d = b_{d-1} A_{d-1} + a_d A_d.$$

令 $v_0(x) = 1$, $v_1(x) = x$. 如下递归地定义 $v_i(x)$:

$$\begin{aligned} xv_i(x) &= b_{i-1} v_{i-1}(x) + a_i v_i(x) + c_{i+1} v_{i+1}(x), \\ xv_d(x) &= b_{d-1} v_{d-1}(x) + a_d v_d(x) + v_{d+1}(x) \end{aligned}$$

(注意到 $c_i \neq 0$). 于是我们有 $A_i = v_i(A_1)\,(i = 0, 1, \cdots, d)$ 及 $v_{d+1}(A_1) = 0$. 这样, A_1 生成一个 $d+1$ 维的交换代数, 具有基 $A_0, A_1, \cdots, A_d$. 注意到 $A_0, A_1, \cdots, A_d$ 都是 (0, 1) 矩阵, 并且 1.1 中的条件 (i)′~(v)′ 被满足, 所以 $\mathfrak{X} = (X, \{R_i\}_{0 \leqslant i \leqslant d})$ 是一个对称结合方案, 于是 Γ 是距离正则的. □

(1.39) 中的数 c_i, a_i, b_i 叫做距离正则图 Γ 的参数. 从定理 1.24 可知, 距离正则图 Γ 确定的结合方案是 P 多项式的; 反之 P 多项式结合方案中由 R_1 确定的图是距离正则的.

关于 P 多项式结合方案的一些参数的性质有下面的

定理 1.25 设 $\mathfrak{X} = (X, \{R_i\}_{0 \leqslant i \leqslant d})$ 是一个关于顺序 $R_0, R_1, \cdots, R_d$ 的 P 多项式结合方案, 并设

$$B_1 = (p^j_{1i}) = \left\{ \begin{matrix} * & 1 & c_2 & \cdots & c_{d-1} & c_d \\ 0 & a_1 & a_2 & \cdots & a_{d-1} & a_d \\ k & b_1 & b_2 & \cdots & b_{d-1} & * \end{matrix} \right\}$$

是关于 R_1 的交叉矩阵, k_i 为 R_i 的价且 $k = k_1$. 再设 $\theta_0 = k, \theta_1, \cdots, \theta_d$ 为 B_1 的特征值. 那么

(i) $a_i + b_i + c_i = k\,(0 \leqslant i \leqslant d)$, 而 $c_0 = b_d = 0$,

(ii) $k_i = k\frac{b_1 b_2 \cdots b_{i-1}}{c_2 c_3 \cdots c_i}$ $(2 \leqslant i \leqslant d)$,

(iii) $k \geqslant b_1 \geqslant b_2 \geqslant \cdots \geqslant b_{d-1}$,

(iv) $1 \leqslant c_2 \leqslant c_3 \leqslant \cdots \leqslant c_d$,

(v) 存在 i_0使得

$$k_0 \leqslant k_1 \leqslant \cdots \leqslant k_{i_0} \geqslant k_{i_0+1} \geqslant k_{i_0+2} \geqslant \cdots \geqslant k_d,$$

(vi) $\theta_0, \theta_1, \cdots, \theta_d$ 是不同的实数, 并且 $-k \leqslant \theta_i \leqslant k\,(0 \leqslant i \leqslant d)$.

证明 (i) 由命题 1.1(v) 知 $\sum_{j=0}^{d} p^i_{1j} = k_1$. 现在 $a_i = p^i_{1i}$, $b_i = p^i_{1i+1}$, $c_i = p^i_{1i-1}$, 而 $p^i_{1j} = 0$ 当 $|j-i| \geqslant 2$. 于是 $a_i + b_i + c_i = k_1$.

(ii) 由命题 1.1(vi) 知 $k_i p^i_{1j} = k_j p^j_{1i}$(因 $\mathfrak{X}$ 对称), 于是有 $k_i p^i_{1i-1} = k_{i-1} p^{i-1}_{1i}$, 即 $k_i c_i = k_{i-1} b_{i-1}$. 因此 $k_i = k_{i-1} b_{i-1}/c_i$, 所以

$$k_i = k_{i-1} b_{i-1}/c_i = \cdots = k b_1 b_2 \cdots b_{i-1}/c_2 c_3 \cdots c_i.$$

(iii) 令 $\Gamma = (X, R_1)$ 为顶点集为 X 而边集为 R_1 的图, 它是距离正则的. 取顶点 x 和 y 使得 $\partial(x, y) = i$. 那么

$$b_i = p^i_{1 i+1} = |\Gamma(x) \cap \Gamma_{i+1}(y)|.$$

取定 $z \in \Gamma_{i-1}(x) \cap \Gamma(y)$. 对于任意 $w \in \Gamma(x) \cap \Gamma_{i+1}(y)$, 我们断言: $\partial(w, z) = i$. 考虑三角形 xwz 可知 $\partial(w, z) \leqslant i$. 再考虑三角形 wyz 可知 $\partial(w, z) \geqslant i$, 于是 $\partial(w, z) = i$. 这就是说 $w \in \Gamma(x) \cap \Gamma_i(z)$, 即

$$\Gamma(x) \cap \Gamma_{i+1}(y) \subseteq \Gamma(x) \cap \Gamma_i(z)$$

(注意 $\partial(x, y) = i$, $\partial(x, z) = i - 1$). 于是立得 $b_i \leqslant b_{i-1}$. (iii) 得证.

(iv) 取定 x, y 使 $\partial(x, y) = i$. 那么

$$c_i = p^i_{1\, i-1} = |\Gamma(x) \cap \Gamma_{i-1}(y)|.$$

取定 $z \in \Gamma_{i+1}(x) \cap \Gamma(y)$. 对于任 $w \in \Gamma(x) \cap \Gamma_{i-1}(y)$, 考虑三角形 xwz 和三角形 wyz 立得 $\partial(w, z) = i$. 于是就有

$$\Gamma(x) \cap \Gamma_{i-1}(y) \subseteq \Gamma(x) \cap \Gamma_i(z).$$

注意到 $\partial(x, y) = i$, $\partial(x, z) = i + 1$, 立得 $c_i \leqslant c_{i+1}$. (iv) 得证.

(v) 由 $k_i = \frac{c_{i+1}}{b_i} k_{i+1} = \frac{b_{i-1}}{c_i} k_{i-1}$ 且 $c_i \leqslant c_{i+1}$, $b_i \leqslant b_{i-1}$ 就有 $k_i^2 \geqslant k_{i-1} k_{i+1}$. 因而有

$$\frac{k_{i-1}}{k_i} \leqslant \frac{k_i}{k_{i+1}}.$$

于是存在 i_0 使得

$$\frac{k_{i_0-1}}{k_{i_0}} \leqslant 1 \leqslant \frac{k_{i_0}}{k_{i_0+1}}.$$

(vi) 由定理 1.23, 特征值 $p_i(j) = v_i(\theta_j)$, 这里 $v_i(x)$ 是 i 次多项式. 于是 $\mathfrak{X}$ 的第一特征值矩阵 $P = (v_i(\theta_j))$. 因为 P 是非奇异的, 所以 $\theta_0, \theta_1, \cdots, \theta_d$ 两两不等. 又因为 A_1 是对称矩阵, 而这些 θ_j 都是 A_1 的特征值, 所以 $\overline{\theta}_j = \theta_j$.

由命题 1.8(i) 知 $k_i = p_i(0)$, 所以 $k_i = v_i(\theta_0) = v_i(k)$. 再由 (1.15) 知 $(k_0, k_1, \cdots, k_d)$ 是 ${}^tB_1$ 的属于特征值 k 的特征向量. 设 θ 为 ${}^tB_1$ 的一个特征值, $\mathbb{X}$ 为 ${}^tB_1$ 的特征向量, 属于特征值 θ, 即 $\mathbb{X}\,{}^tB_1 = \theta\mathbb{X}$. 设 $\mathbb{X}$ 的分量均非负, 那么 $\theta \geqslant 0$. 现在令 $\mathbb{X}_0 = (k_0, k_1, \cdots, k_d)$, 再取 $c > 0$ 极大而使 $\mathbb{X}_0 - c\mathbb{X}$ 的每个分量均为非负, 那么由 $(\mathbb{X}_0 - c\mathbb{X})\,{}^tB_1 = k(\mathbb{X}_0 - \frac{\theta}{k}c\mathbb{X})$ 推出 $\mathbb{X}_0 - \frac{\theta}{k}c\mathbb{X}$ 的分量均非负, 再由 c 的极大性立得 $\frac{\theta}{k} \leqslant 1$, 即 $\theta \leqslant k$. 设 $\mathbb{X}$ 有正分量也有负分量, 取 $|c|$ 极大而使 $\mathbb{X}_0 - c\mathbb{X}$ 是非负的, 那么 $(\mathbb{X}_0 - c\mathbb{X})\,{}^tB_1$ 非负, 推出 $\mathbb{X}_0 - \frac{\theta}{k}c\mathbb{X}$ 非负. 再由 $|c|$ 的极大性立得 $|\frac{\theta}{k}| \leqslant 1$, 即 $-k \leqslant \theta \leqslant k$. □

最后, 我们介绍 Q 多项式结合方案的概念. 设 $\mathfrak{X}=(X,\{R_i\}_{0\leqslant i\leqslant d})$ 是一个对称结合方案, $E_i\,(0\leqslant i\leqslant d)$ 是邻接代数 $\mathfrak{A}$ 的本原幂等元. $\mathfrak{X}$ 叫做关于顺序 $E_0, E_1, \cdots, E_d$ 的 *Q多项式结合方案*, 如果存在 i 次多项式 $v_i^*(x)$ 使得 $E_i=v_i^*(E_1)$ $(i=0,1,\cdots,d)$, 这里的乘法是 Hadamard 乘法 (实际上可以证明 $v_i(x)$ 的系数均为实数). 设 q_{ij}^k 是 $\mathfrak{X}$ 的 Krein 参数, $\widehat{B}_1=(q_{1i}^j)$, 并令 $Q=(q_i(j))$ 为 $\mathfrak{X}$ 的第二特征值矩阵. 那么有

定理 1.26 设 $\mathfrak{X}=(X,\{R_i\}_{0\leqslant i\leqslant d})$ 是对称结合方案, 那么下面的 (i), (ii), (iii) 彼此等价:

(i) $\mathfrak{X}$ 是关于顺序 $E_0, E_1, \cdots, E_d$ 的 Q 多项式方案, 即存在 i 次多项式 $v_i^*(x)$ 使得

$$E_i=v_i^*(E_1)\ (i=0,1,\cdots,d),$$

这里的乘法是 Hadamard 乘法.

(ii) 存在 i 次多项式 $v_i^*(x)$ 使得 $Q=(q_i(j))$ 满足

$$\begin{aligned} q_i(j)&=v_i^*(\theta_j^*)\ (i,j=0,1,\cdots,d),\\ \theta_j^*&=q_1(j)\ (j=0,1,\cdots,d). \end{aligned}$$

(iii) $\widehat{B}_1=(q_{1i}^j)$ 是三对角线矩阵, 其旁对角线元素不为零, 即

$$\widehat{B}_1=(q_{1i}^j)=\left\{\begin{array}{cccccc} * & 1 & c_2^* & \cdots & c_{d-1}^* & c_d^* \\ 0 & a_1^* & a_2^* & \cdots & a_{d-1}^* & a_d^* \\ m & b_1^* & b_2^* & \cdots & b_{d-1}^* & * \end{array}\right\},$$

这里 $m=m_0$.

证明 仿定理 1.23 的证明. □

如果结合方案 $\mathfrak{X}$ 既是 P 多项式的, 又是 Q 多项式的, 那么 $\mathfrak{X}$ 就叫做*(P 和 Q) 多项式方案*. 本书下面讨论的结合方案有的就是 (P 和 Q) 多项式方案.

§1.9 结合方案的自同构

设 Γ 和 Γ' 是两个 (有向) 图, 其顶点集分别是 X 和 X', 边集分别是 R 和 R'. 设 $|X|=|X'|$. f 是从 X 到 X' 的一个 1-1 映射, 如果对于 X 的任意一对顶点 x 和 y 有 $(x,y)\in R$ 当且仅当 $(f(x),f(y))\in R'$, 那么称 f 是从图 Γ 到图 Γ' 的一个同构. 这时称图 Γ 和图 Γ' 是同构的.

如果 f 是图 Γ 到它自身的同构, 那么就称 f 是图 Γ 的一个自同构. 图 Γ 的全体自同构对于映射的乘法 (合成) 作成一个群, 叫做图 Γ 的自同构群, 记作 $\mathrm{Aut}\Gamma$.

现在设 $\mathfrak{X} = (X, \{R_i\}_{0\leqslant i\leqslant d})$ 和 $\mathfrak{X}' = (X', \{R'\}_{0\leqslant i\leqslant d})$ 是两个结合方案, 它们的类数相等. 设 $|X| = |X'|$, f 是从 X 到 X' 的一个 1–1 映射并且诱导出 $\{0, 1, \cdots, d\}$ 上的一个置换 $\sigma(f)$, 就是说, 对于 X 的任意一对顶点 x 和 y 均有 $(x, y) \in R_i$ 当且仅当 $(f(x), f(y)) \in R'_{i^{\sigma(f)}}$, 那么称 f 是结合方案 $\mathfrak{X}$ 到结合方案 $\mathfrak{X}'$ 的一个同构. 这时称结合方案 $\mathfrak{X}$ 和结合方案 $\mathfrak{X}'$ 是同构的.

如果 f 是结合方案 $\mathfrak{X}$ 到它自身的同构, 那么就称 f 是结合方案 $\mathfrak{X}$ 的一个自同构. $\mathfrak{X}$ 的全体自同构对于映射的合成作成一个群, 叫做结合方案的自同构群, 记作 $\mathrm{Aut}\,\mathfrak{X}$.

设 $f \in\mathrm{Aut}\,\mathfrak{X}$, 即 f 是结合方案 $\mathfrak{X} = \{X, \{R_i\}_{0\leqslant i\leqslant d}\}$ 的一个自同构. 如果 f 诱导出 $\{0, 1, \cdots, d\}$ 上的置换 $\sigma(f)$ 是恒等置换, $i^{\sigma(f)} = i$, $i = 0, 1, \cdots, d$, 那么称 f 是 $\mathfrak{X}$ 的一个内自同构. 显然, $\mathfrak{X}$ 的全体内自同构作成 $\mathrm{Aut}\,\mathfrak{X}$ 的一个子群, 记作 $\mathrm{Inn}\,\mathfrak{X}$. 易见,$\mathrm{Inn}\,\mathfrak{X}$ 是 $\mathrm{Aut}\,\mathfrak{X}$ 的一个正规子群. 商群 $\mathrm{Aut}\mathfrak{X}/\mathrm{Inn}\mathfrak{X}$ 叫做 $\mathfrak{X}$ 的外自同构群.

又显然有,$\mathrm{Inn}\,\mathfrak{X} = \cap_{i=1}^{d}\mathrm{Aut}\,\Gamma^{(i)}$, 这里 $\Gamma^{(i)}$ 为结合关系 R_i 的图.

定理 1.27 设 $\mathfrak{X} = (X, \{R_i\}_{0\leqslant i\leqslant d})$ 和 $\mathfrak{X}' = (X', \{R'_i\}_{0\leqslant i\leqslant d})$ 是两个结合方案, p'^{k}_{ij}, k'_i 为 X' 的交叉数和价, f 是 $\mathfrak{X}$ 到 $\mathfrak{X}'$ 的一个同构, $\sigma(f)$ 是 f 诱导出 $\{0, 1, \cdots, d\}$ 上的置换. 那么有

$$p^k_{ij} = p'^{k^{\sigma(f)}}_{i^{\sigma(f)}\, j^{\sigma(f)}},\ \forall i,\ j,\ k \in \{0,\ 1,\ \cdots,\ d\}.$$

因此, $\mathfrak{X}$ 交换 (对称) 当且仅当 $\mathfrak{X}'$ 交换 (对称). 特别有

$$k_i = k'_{i^{\sigma(f)}},\ i = 0,\ 1,\ \cdots,\ d. \tag{1.41}$$

证明 任取 $x, y \in X$ 使 $(x, y) \in R_k$. 那么 $x^f, y^f \in X'$ 有 $(x^f, y^f) \in R'_{k^{\sigma(f)}}$. 于是

$$\begin{aligned} p^k_{ij} =&\ |\{z \in X|(x, z) \in R_i, (z, y) \in R_j\}| \\ =&\ |\{z^f \in X'|(x^f, z^f) \in R'_{i^{\sigma(f)}}, (z^f, y^f) \in R'_{j^{\sigma(f)}}\}| = p'^{k^{\sigma(f)}}_{i^{\sigma(f)}\, j^{\sigma(f)}}. \end{aligned}$$

特别是由于 $\sigma(f)$ 使 0 不动, 我们就有 $k_i = p^0_{ii'} = p'^0_{i^{\sigma(f)}\, i^{\sigma(f)\prime}} = k'_{i^{\sigma(f)}}$. □

推论 1.28 (i) 设结合方案 $\mathfrak{X} = (X, \{R_i\}_{0\leqslant i\leqslant d})$ 的价 $k_i\,(i = 1, \cdots, d)$ 两两不等, 那么

$$\mathrm{Aut}\,\mathfrak{X} = \mathrm{Inn}\,\mathfrak{X}.$$

(ii) 如果 $\mathfrak{X}$ 关于顺序 $R_0, R_1, \cdots, R_d$ 是 P 多项式的, 那么

$$\mathrm{Inn}\,\mathfrak{X} = \mathrm{Aut}\,\Gamma^{(1)}.$$

证明 (i) 由于 $k_1, \cdots, k_d$ 两两不等, 那么每个自同构 f 诱导出 $\{0, 1, \cdots, d\}$ 上的置换 $\sigma(f)$ 必为恒等置换 (因 (1.41)), 所以 $f \in \operatorname{Inn}\mathfrak{X}$.

(ii) 对于 $(x, y) \in R_i$, 它们在图 $\Gamma^{(1)}$ 中的距离为 i, 每个 $f \in \operatorname{Aut}\Gamma^{(1)}$ 保持图 $\Gamma^{(1)}$ 中任二点间的距离, 所以 $(x^f, y^f) \in R_i$. 于是 f 也是图 $\Gamma^{(i)}$ 的自同构, 即 $\operatorname{Aut}\Gamma^{(1)} \subseteq \operatorname{Aut}\Gamma^{(i)}$. 于是立得 $\operatorname{Aut}\Gamma^{(1)} = \operatorname{Inn}\mathfrak{X}$. □

第二章　长方矩阵的结合方案

§2.1　长方阵结合方案的构作及其本原性

令 $\mathbb{F}_q$ 表示 q 元有限域, 这里 q 是一个素数 p 的幂. 设 m 和 n 为两个正整数, 不妨设 $m \leqslant n$. 令 $M_{mn}(\mathbb{F}_q)$ 表示 $\mathbb{F}_q$ 上全体 $m\times n$ 矩阵的集合, 它关于矩阵加法作成一个加法群. 如果再考虑到 $\mathbb{F}_q$ 中的元素对矩阵的纯量乘法, 那么 $M_{mn}(\mathbb{F}_q)$ 作成 $\mathbb{F}_q$ 上的一个向量空间. 令 E_{ij} 表示 (i,j) 位置元素为 1 而其余元素为 0 的 $m\times n$ 矩阵, $\{E_{ij}|1\leqslant i\leqslant m,\ 1\leqslant j\leqslant n\}$ 作成 $M_{mn}(\mathbb{F}_q)$ 的一组基, 因此 $\dim M_{mn}(\mathbb{F}_q)=mn$. 为了书写方便, 将 $M_{mn}(\mathbb{F}_q)$ 简单记作 M_{mn}.

令 $G_0=GL_m(\mathbb{F}_q)\times GL_n(\mathbb{F}_q)$(直积), G_0 如下作用在 M_{mn} 上:

$$\begin{aligned} M_{mn}\times G_0 &\longrightarrow M_{mn} \\ (X,\,(P,Q)) &\longmapsto PXQ. \end{aligned} \tag{2.1}$$

显然, $(P,\,Q)$ 给出加法群 M_{mn} 的一个自同构. 这个作用是 G_0 在向量空间 M_{mn} 上一个线性表示, 其核为 $\{(aI^{(m)},\,a^{-1}I^{(n)})|a\in\mathbb{F}_q,\,a\neq 0\}$. 令 T_0 表示加法群 M_{mn} 的平移群, 再设 G 是由 G_0 和 T_0 生成的群. G 可迁地作用在加法群 M_{mn} 上, 于是由定理 1.3, $(G,\,M_{mn})$ 决定 M_{mn} 上的一个交换结合方案, 记作 $\mathrm{Mat}(m\times n,\,q)$.

显然 $|M_{mn}|=q^{mn}$. 由定理 1.4 知, 这个结合方案的类数等于 G_0 在 M_{mn} 上的非平凡轨道数. M_{mn} 中两个矩阵 X 和 Y 在同一个 G_0 轨道当且仅当存在 $P\in GL_m(\mathbb{F}_q)$, $Q\in GL_n(\mathbb{F}_q)$ 使得 $PXQ=Y$, 即当且仅当 X 和 Y 有相等的秩, 因此, 结合方案 $\mathrm{Mat}(m\times n,q)$ 的类数为 m. 令

$$C_i=\{X\in M_{mn}|\mathrm{rank}\,X=i\},\ i=0,\,1,\,\cdots,\,m.$$

那么相应的结合类为

$$R_i=\{(X,\,Y)\in M_{mn}\times M_{mn}|Y-X\in C_i\},\ i=0,\,1,\,\cdots,\,m.$$

由于 $\mathrm{rank}\,(Y-X)=\mathrm{rank}\,(X-Y)$, 所以结合方案 $\mathrm{Mat}(m\times n,q)$ 是对称的. 结合关系 R_i 的价 k_i 恰为 M_{mn} 中秩为 i 的矩阵个数, 记作 $n_i(m\times n,\,q)$. 熟知 (参见 [15])

$$|GL_m(\mathbb{F}_q)|=q^{\frac{1}{2}m(m-1)}\prod_{j=1}^{m}(q^j-1). \tag{2.2}$$

对于 $n_i(m\times n,q)$, 我们有下面的计数公式.

定理 2.1 设 $m\leqslant n$. $\mathbb{F}_q$ 上秩为 i 的 $m\times n$ 矩阵个数

$$n_i(m\times n,\,q)=q^{\frac{1}{2}i(i-1)}\frac{\prod\limits_{j=m-i+1}^{m}(q^j-1)\prod\limits_{j=n-i+1}^{n}(q^j-1)}{\prod\limits_{j=1}^{i}(q^j-1)}. \tag{2.3}$$

证明 考虑

$$M_i=\begin{pmatrix} I^{(i)} & 0\\ 0 & 0\end{pmatrix}\begin{matrix} i\\ m-i\end{matrix}\in C_i$$
$$\qquad\quad\ \ i\qquad n-i$$

在 G_0 中的稳定子 G_{M_i}. 设 $(P,\,Q)\in G_0$. 将 P,Q 适当分块, 写为

$$P=\begin{pmatrix} A & B\\ C & D\end{pmatrix}\begin{matrix} i\\ m-i\end{matrix},\ Q=\begin{pmatrix} U & V\\ W & Z\end{pmatrix}\begin{matrix} i\\ n-i\end{matrix}.$$
$$\quad i\quad m-i\qquad\qquad\quad i\quad n-i$$

那么 $PM_iQ=M_i$ 当且仅当 $AU=I^{(i)}$, $C=0$, $V=0$, $D\in GL_{m-i}(\mathbb{F}_q)$ 及 $Z\in GL_{n-i}(\mathbb{F}_q)$. 由于 C_i 是一个 G_0 轨道, 因此

$$|C_i|=\frac{|G_0|}{|G_{M_i}|}=\frac{|GL_m(\mathbb{F}_q)|\,|GL_n(\mathbb{F}_q)|}{|GL_i(\mathbb{F}_q)|\,|GL_{m-i}(\mathbb{F}_q)|\,|GL_{n-i}(\mathbb{F}_q)|\,q^{i(m-i)+i(n-i)}}.$$

利用关于一般线性群的阶的公式 (2.2) 将上式整理即得 (2.3). □

令 $\Gamma^{(i)}$ $(i\neq 0)$ 表示结合关系 R_i 的图, 即图 $\Gamma^{(i)}$ 的顶点集为 M_{mn}, 它的边集为 R_i. 由于 R_i 是对称的, 所以 $\Gamma^{(i)}$ 是无向图. 下面我们证明结合方案 $\mathrm{Mat}(m\times n,\,q)$ 的关系图都是连通的. 由定理 1.18 可知, 只要证明群 G 在 M_{mn} 上的作用是本原的. 为此, 我们先证明下面的

定理 2.2 群 G_0 在 M_{mn} 上的表示 (2.1) 是不可约的, 就是说, 除了 0 和 M_{mn} 外, 没有 G_0 不变子空间.

证明 设 W 是 M_{mn} 的一个 G_0 不变子空间, 且 $W\neq\{0\}$. 往证 $W=M_{mn}$.

由于 $W\neq\{0\}$, 任取 W 中的一个矩阵 $A\neq 0$. 设 $\operatorname{rank}A=r>0$. 因为 W 是 G_0 不变的, 即对任意 $P\in GL_m(\mathbb{F}_q)$ 和任意 $Q\in GL_n(\mathbb{F}_q)$ 均有 $PAQ\in W$, 于是 W 包有 M_{mn} 中全体秩为 r 的矩阵. 如果 $r=1$, 那么 W 包有 M_{mn} 中全体秩为 1 的矩阵. 由于 M_{mn} 中每个非零矩阵均可表为若干个秩为 1 的矩阵之和, 于是 M_{mn} 中每个矩阵均在 W 中, 即 $W=M_{mn}$.

设 $r>1$. W 包有如下两个秩为 r 的矩阵

$$A_1=[I^{(r)},\,0^{(m-r,n-r)}],\ A_2=\left[\begin{pmatrix}-1 & 0\\ 1 & -1\end{pmatrix},\,-I^{(r-2)},\,0^{(m-r,n-r)}\right].$$

于是 W 也包有它们的和 A_1+A_2, 而 $\operatorname{rank}(A_1+A_2)=1$, 这就归结到 $r=1$ 的情形. □

定理 2.3　群 G 作用在 M_{mn} 上是本原的.

证明　注意到 G 中的元素可表示成 $((P, Q), A)$, 它在 M_{mn} 上的作用为

$$X \longrightarrow PXQ+A.$$

于是 G 中两个元素 $((P_1, Q_1), A_1)$ 和 $((P_2, Q_2), A_2)$ 的乘积为

$$((P_1, Q_1), A_1)((P_2, Q_2), A_2)=((P_2P_1, Q_1Q_2), P_2A_1Q_2+A_2).$$

由定理 1.19, G 在 M_{mn} 上的作用是本原的当且仅当 M_{mn} 的任一元素 X 在 G 中的稳定子 G_X 均是 G 的极大子群. 现在取 $X=0$, 它在 G 中的稳定子恰为 G_0. 我们证明 G_0 是 G 的一个极大子群. 设 H 是 G 的一个子群使得 $G_0 \subsetneq H \subseteq G$, 往证 $H=G$. 令

$$W=\{A \in M_{mn} | \text{存在}\,(P, Q) \in G_0\,\text{使得}\,((P, Q), A) \in H\}.$$

由于 $G_0 \subsetneq H$, $W \neq \{0\}$. 任取 $A \in W$, $((P_1, Q_1), A) \in H$. 对于任意 $(P, Q) \in G_0$ 有

$$((P_1, Q_1), A)((P, Q), 0)=((PP_1, Q_1Q), PAQ) \in H.$$

于是 $PAQ \in W$, 即 W 是 G_0 不变的. 取 $P=aI^{(m)}$, $Q=I^{(n)}$, $a \in \mathbb{F}_q$, $a \neq 0$, 可知 W 对于 $\mathbb{F}_q$ 的纯量乘法是封闭的. 注意到

$$((P_1^{-1}, Q_1^{-1}), 0)((P_1, Q_1), A)=((I^{(m)}, I^{(n)}), A) \in H.$$

对于 W 中的任意两个元素 A, B, 就有 $((I^{(m)}, I^{(n)}), A) \in H$ 和 $((I^{(m)}, I^{(n)}), B) \in H$, 而 $((I^{(m)}, I^{(n)}), A)((I^{(m)}, I^{(n)}), B)=((I^{(m)}, I^{(n)}), A+B) \in H$, 所以 $A+B \in W$. 这就是说 W 是一个 G_0 不变的子空间. 由定理 2.2, G_0 在 M_{mn} 上是不可约的, 于是 $W=M_{mn}$, 因而 $H=G$. 这就证明了本定理. □

由定理 2.3 和定理 1.18, 我们就有

定理 2.4　长方阵结合方案 $\mathrm{Mat}(m \times n, q)$ 是本原的, 因而它的结合关系图 $\Gamma^{(i)}$ $(i=1, \cdots, m)$ 都是连通的.

§2.2　长方阵结合方案的 P 多项式性质

我们知道, 结合方案 $\mathrm{Mat}(m \times n, q)$ 的结合关 R_i 是群 G 作用在 $M_{mn} \times M_{mn}$ 上的轨道. 因此 G 可看作结合关系图 $\Gamma^{(i)}$ 的一个自同构群. 由定理 2.4 知道长方阵

结合方案的结合关系图 $\Gamma^{(i)}$ $(i \neq 0)$ 都是连通的. 在这一节中, 我们主要讨论结合关系图 $\Gamma^{(1)}$.

$\Gamma^{(1)}$ 是这样的一个图, 它以 $\mathbb{F}_q$ 上全体 $m\times n$ 矩阵作为顶点, 两顶点 X 和 Y 邻接当且仅当 $\operatorname{rank}(Y-X)=1$. 在文献中, 这个图也记作 $\operatorname{Bil}(m\times n,\, q)$, 即双线性形式的图. 我们用 ∂ 表示图 $\Gamma^{(1)}$ 的距离函数. $\partial(X, Y)$ 表示两个顶点 X 和 Y 之间的距离, 即连接 X 和 Y 的最短道路之长 (参考 §1.6). 设

$$X=X_0,\, X_1,\, \cdots,\, X_{s-1},\, X_s=Y$$

是顶点 X 和 Y 间的一条长为 s 的道路, 即依次相邻两点邻接, 即 $\operatorname{rank}(X_i-X_{i-1})=1$, $i=1,\cdots,s$. 由线性代数知, 矩阵和的秩不超过各和项的秩之和, 于是我们有

$$s=\operatorname{rank}(X_1-X_0)+\operatorname{rank}(X_2-X_1)+\cdots+\operatorname{rank}(X_s-X_{s-1})\geqslant \operatorname{rank}(Y-X).$$

特别地, 我们就有 $\operatorname{rank}(Y-X)\leqslant \partial(X, Y)$.

现在我们证明上式中等号成立. 设 $\operatorname{rank}(Y-X)=r>0$. 由于群 G 的任一元素 $((P, Q), A)$ 保持两矩阵差之秩, 即

$$\operatorname{rank}((PYQ+A)-(PXQ+A))=\operatorname{rank}P(Y-X)Q=\operatorname{rank}(Y-X).$$

因而保持两点间的距离, 于是不妨设

$$X=0,\ Y=[I^{(r)},\, 0^{(m-r,n-r)}]. \tag{2.4}$$

我们令

$$Y_j=[I^{(j)},\, 0^{(m-j,n-j)}],\ j=0,\, 1,\, \cdots,\, r.$$

那么 $\operatorname{rank}(Y_j-Y_{j-1})=1, j=1,\cdots,r$, 即 $Y_0=X, Y_1, Y_2,\cdots, Y_r=Y$ 是 X 和 Y 间的一条长为 r 的道路, 于是有 $\partial(X, Y)\leqslant r=\operatorname{rank}(Y-X)$. 这样我们得到

定理 2.5 对于关系图 $\Gamma^{(1)}$ 来说, 恒有

$$\partial(X, Y)=\operatorname{rank}(X-Y).$$

设 Γ 是一个连通图, (x, y) 和 (x_1, y_1) 是 Γ 的任意两对顶点, 如果它们之间距离相等, 总存在 Γ 的一个自同构 σ 使得 $x^\sigma=x_1$, $y^\sigma=y_1$, 那么就称这个图 Γ 是距离可迁的. 由定理 1.24 可知, 如果 Γ 是连通的, 并且是距离可迁的, 那么 Γ 一定是距离正则的. 对于我们的结合关系图 $\Gamma^{(1)}$ 来说, 我们有下面的

定理 2.6 结合关系图 $\Gamma^{(1)}$ 是距离可迁的, 因而 $\Gamma^{(1)}$ 是距离正则的.

证明 设 $(0, Y)$ 是形如 (2.4) 的两个顶点, 于是 $\partial(0, Y)=r$. 设 (A, B) 是 $\Gamma^{(1)}$ 的任一对顶点而有 $\partial(A, B)=r$. 现在 G 中元素 $((I^{(m)}, I^{(n)}), -A)$ 将 A 变到 0, 而将

B 变到 $B-A$. 由于 $\mathrm{rank}\,(B-A)=\partial(A,B)=r$, 存在 $P\in GL_m(\mathbb{F}_q)$, $Q\in GL_n(\mathbb{F}_q)$ 使得 $P(B-A)Q=Y$. 因此有 $\Gamma^{(1)}$ 的自同构 $((P,Q),-PAQ)$ 将顶点对 (A,B) 变到顶点对 $(0,Y)$. 这就证明了 $\Gamma^{(1)}$ 是距离可迁的, 因而 $\Gamma^{(1)}$ 是距离正则的. □

由定理 2.6 和定理 1.23, 立得

定理 2.7　设 $m\leqslant n$. 长方阵结合方案 $\mathrm{Mat}(m\times n,q)$ 关于顺序 $R_0, R_1, \cdots, R_m$ 是 P 多项式的.

现在, 我们计算距离正则图 $\Gamma^{(1)}$ 的参数, 由定理 2.1 知 $\Gamma^{(1)}$ 的价为

$$k_1=n_1(m\times n,q)=(q^m-1)(q^n-1)/(q-1).$$

下面我们计算 $\Gamma^{(1)}$ 的参数组 $c_i, a_i, b_i\,(i=0,1,\cdots,d)$, 即结合方案 $\mathrm{Mat}\,(m\times n,q)$ 的交叉数 $p^i_{1i-1}, p^i_{1i}, p^i_{1i+1}$. M_{mn} 中每个秩为 1 的矩阵 X 均可表为如下形状

$$X={}^tuv,\quad 这里\, u=(x_1,\cdots,x_m)\in\mathbb{F}_q^{(m)},\ v=(y_1,\cdots,y_n)\in\mathbb{F}_q^{(n)}, \tag{2.5}$$

且 $u\neq 0$ 和 $v\neq 0$. 如果 $X={}^tu_1v_1$, 那么存在 $a\in\mathbb{F}_q$, $a\neq 0$ 使得 $u_1=au$, $v_1=a^{-1}v$.

设 B, A 是 $\Gamma^{(1)}$ 的两个顶点, 而有 $\partial(B,A)=i$, 那么

$$\begin{aligned} c_i=p^i_{1\,i-1}&=|\Gamma^{(1)}_{i-1}(A)\cap\Gamma^{(1)}(B)|,\\ a_i=p^i_{1\,i}\ &=|\Gamma^{(1)}_{i}(A)\cap\Gamma^{(1)}(B)|,\\ b_i=p^i_{1\,i+1}&=|\Gamma^{(1)}_{i+1}(A)\cap\Gamma^{(1)}(B)|. \end{aligned}$$

考虑到 R_1 是 G 轨道, 因而 G 保持 $\Gamma^{(1)}$ 的顶点间之距离. 于是由定理 2.5 知, 不失一般性, 我们可设

$$B=0\ 及\ A=[I^{(i)},\,0^{(m-i,n-i)}]. \tag{2.6}$$

设 $X\in M_{mn}$ 且 $\mathrm{rank}\,X=1$. 于是可设 $X={}^tuv$, $u\neq 0$, $v\neq 0$(见 (2.5)). 将 u, v 相应 (2.6) 中 A 的形状分块, 写 $u=(u_1,u_2)$, $v=(v_1,v_2)$, 这里

$$u_1=(x_1,\cdots,x_i), u_2=(x_{i+1},\cdots,x_m), v_1=(y_1,\cdots,y_i), v_2=(y_{i+1},\cdots,y_n).$$

我们观察 $\mathrm{rank}\,(A+X)$. 区别下面几种情形讨论之.

a) 设 $u_2\neq 0$ 和 $v_2\neq 0$. 那么存在 $P\in GL_m(\mathbb{F}_q)$ 和 $Q\in GL_n(\mathbb{F}_q)$ 使得

$$P(A+X)Q=P\left(\begin{array}{c|c} I^{(i)}+{}^tu_1v_1 & {}^tu_1v_2\\ \hline {}^tu_2v_1 & {}^tu_2v_2\end{array}\right)Q=[I^{(i)},\,1,\,0^{(m-i-1,n-i-1)}].$$

对于这样的 X 有 $\mathrm{rank}\,(A+X)=i+1$, 它的个数为 $q^{2i}(q^{m-i}-1)(q^{n-i})/(q-1)$.

b) 设 $u_2=0$ 而 $v_2\neq 0$. 这时 $u_1\neq 0$, 于是存在 $P\in GL_m(\mathbb{F}_q)$ 和 $Q\in GL_n(\mathbb{F}_q)$ 使得

$$P(A+X)Q=P\left(\begin{array}{c|c} I^{(i)}+{}^tu_1v_1 & {}^tu_1v_2 \\ \hline 0 & 0 \end{array}\right)Q=\left(\begin{array}{c|c} I^{(i)} & {}^tu_1v_2 \\ \hline 0 & 0 \end{array}\right).$$

对于这样的 X 有 $\operatorname{rank}(A+X)=i$, 它的个数为 $q^i(q^i-1)(q^{n-i}-1)/(q-1)$.

同理, 设 $u_2\neq 0$ 而 $v_2=0$. 这时 $v_1\neq 0$, 那么存在 $P\in GL_m(\mathbb{F}_q)$ 和 $Q\in GL_n(\mathbb{F}_q)$ 使得

$$P(A+X)Q=P\left(\begin{array}{c|c} I^{(i)}+{}^tu_1v_1 & 0 \\ \hline {}^tu_2v_1 & 0 \end{array}\right)Q=\left(\begin{array}{c|c} I^{(i)} & 0 \\ \hline {}^tu_2v_1 & 0 \end{array}\right).$$

对于这样的 X 也有 $\operatorname{rank}(A+X)=i$, 它的个数为 $q^i(q^i-1)(q^{m-i}-1)/(q-1)$.

c) 设 $u_2=0$ 和 $v_2=0$. 于是 $u_1\neq 0$, $v_1\neq 0$, 并且

$$A+X=\left(\begin{array}{c|c} I^{(i)}+{}^tu_1v_1 & 0 \\ \hline 0 & 0 \end{array}\right).$$

$\operatorname{rank}(A+X)=\operatorname{rank}(I^{(i)}+{}^tu_1v_1)$. 对于 $v_1\neq 0$, 存在 $T\in GL_i(\mathbb{F}_q)$ 使得 $v_1T=e_1=(1,0,\cdots,0)$. 显然, 有 $\operatorname{rank}(I^{(i)}+{}^tu_1v_1)=\operatorname{rank}(I^{(i)}+T^{-1}\,{}^tu_1v_1T)$. 记 $T^{-1}\,{}^tu_1={}^t(z_1,\cdots,z_i)$. 于是

$$I^{(i)}+(T^{-1}\,{}^tu_1)(v_1T)=\begin{pmatrix} 1+z_1 & & & \\ z_2 & 1 & & \\ \vdots & & \ddots & \\ z_i & \cdots & & 1 \end{pmatrix}.$$

因而

$$\operatorname{rank}(I^{(i)}+{}^tu_1v_1)=\begin{cases} i, & \text{如果 } z_1\neq -1, \\ i-1, & \text{如果 } z_1=-1. \end{cases}$$

我们计算 $u_2=0$ 和 $v_2=0$ 而使 $\operatorname{rank}(A+X)=i-1$ 的 X 之个数. v_1 有 q^i-1 个取法, 在取定 v_1 之后, 取 $T\in GL_i(\mathbb{F}_q)$ 使 $v_1T=e_1$, 再令 $u_1=(-1,z_2,\cdots,z_i)\,{}^tT$, u_1 的选取为 q^{i-1} 个. 因而使 $\operatorname{rank}(A+X)=i-1$ 的 X 之个数为 $q^{i-1}(q^i-1)/(q-1)$.

再来计算 $u_2=0$ 和 $v_2=0$ 而使 $\operatorname{rank}(A+X)=i$ 的 X 之个数. v_1 有 q^i-1 个选取. 取定 v_1 之后, 取 $T\in GL_i(\mathbb{F}_q)$ 使 $v_1T=e_1$. 再令 $u_1=(z_1,z_2,\cdots,z_i)\,{}^tT\neq 0$ 且使 $z_1\neq -1$. 当 $z_2=\cdots=z_i=0$ 时 z_1 的选取有 $q-2$ 个, 当 $(z_2,\cdots,z_i)\neq 0$ 时 z_1 的选取为 $q-1$ 个, 所以满足条件的 u_1 之个数 $q-2+(q^{i-1}-1)(q-1)=q^i-q^{i-1}-1$. 因而使 $\operatorname{rank}(A+X)=i$ 的这种 X 之个数为 $(q^i-1)(q^i-q^{i-1}-1)/(q-1)$.

总结上面的讨论, 我们得到

定理 2.8　关系图 $\Gamma^{(1)}$(它是距离正则的) 的参数组为

$$\begin{aligned}
b_i &= q^{2i}(q^{m-i}-1)(q^{n-i}-1)/(q-1), & 0 \leqslant i \leqslant m-1,\\
c_i &= q^{i-1}(q^i-1)/(q-1), & 1 \leqslant i \leqslant m,\\
a_i &= (q^i-1)(q^m+q^n-q^i-q^{i-1}-1)/(q-1), & 0 \leqslant i \leqslant m.
\end{aligned}$$

一般说来, 对于一个 P 多项式结合方案, 考虑 $A_1(A_iA_j)=(A_1A_j)A_i$ 可得如下参数关系式

$$b_{i-1}p^k_{i-1\,j}+a_ip^k_{i\,j}+c_{i+1}p^k_{i+1\,j}=b_{j-1}p^k_{j-1\,i}+a_jp^k_{j\,i}+c_{j+1}p^k_{j+1\,i}.$$

从中解出 $p^k_{i+1\,j}$, 可以递归地计算 $p^k_{i\,j}$(参看 [3]4.1D). 由于我们的矩阵结合方案其元素与构作具有一定特殊性, 可以给出更为有效的递归计算方法.

§2.3　交叉数 p^k_{ij} 的递归计算公式

在这一节中, 我们给出关于长方阵结合方案 $\mathrm{Mat}(m\times n,q)$ 的交叉数 p^k_{ij} 的递归计算方法. 为此, 我们将 $\mathrm{Mat}(m\times n,q)$ 的交叉数记作 $p^k_{ij}\,(m\times n)$. 这样, 对于任意两个正整数 s, t 和 $\mathbb{F}_q$ 上两个 $s\times t$ 矩阵 A_1, A_2 使得 $\mathrm{rank}\,(A_2-A_1)=k$, $p^k_{ij}\,(s\times t)$ 就表示 $\mathbb{F}_q$ 上满足 $\mathrm{rank}\,(X-A_1)=i$ 及 $\mathrm{rank}\,(X-A_2)=j$ 的 $s\times t$ 矩阵 X 的个数.

现在考虑长方阵结合方案 $\mathrm{Mat}(m\times n,q)$ 的交叉数 p^k_{ij}, 设 $0<k<m\leqslant n$. 取定两个 $m\times n$ 矩阵

$$X_1=0 \text{ 和 } X_2=[I^{(k)},\,0^{(m-k,\,n-k)}].$$

令

$$\mathcal{M}^k_{ij}=\{X\in M_{mn}|\mathrm{rank}\,X=i,\ \mathrm{rank}\,(X-X_2)=j\}.$$

于是 $p^k_{ij}=|\mathcal{M}^k_{ij}|$. 对于 $\mathcal{M}^k_{ij}$ 中的任一矩阵 X 做相应于 X_2 的分块

$$X=\begin{pmatrix} U & V\\ L & W\end{pmatrix}\begin{matrix} k\\ m-k\end{matrix}\ . \tag{2.7}$$
$$\qquad\ \ \begin{matrix} k & \quad n-k\end{matrix}$$

群 G_0 中使 X_2 不动的元素 (P,Q) 具有如下形状

$$P=\begin{pmatrix} A & B\\ 0 & D\end{pmatrix}\begin{matrix} k\\ m-k\end{matrix},\quad Q=\begin{pmatrix} A^{-1} & 0\\ Y & Z\end{pmatrix}\begin{matrix} k\\ n-k\end{matrix}, \tag{2.8}$$
$$\begin{matrix} k & \quad m-k\end{matrix}\qquad\qquad\qquad \begin{matrix} k & \quad n-k\end{matrix}$$

这里 $A \in GL_k(\mathbb{F}_q)$, $D \in GL_{m-k}(\mathbb{F}_q)$, B 为 $k \times (m-k)$ 矩阵, $Z \in GL_{n-k}(\mathbb{F}_q)$, Y 为 $(n-k) \times k$ 矩阵. 显然, 这种 (P, Q) 使 X_1 和 X_2 都不动, 因而将集合 $\mathcal{M}_{ij}^k$ 映到 $\mathcal{M}_{ij}^k$. 由于

$$\begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \begin{pmatrix} U & V \\ L & M \end{pmatrix} \begin{pmatrix} A^{-1} & 0 \\ Y & Z \end{pmatrix} = \begin{pmatrix} * & * \\ * & DWZ \end{pmatrix},$$

可知形如 (2.8) 的 (P, Q) 使 W 的秩不变. 令

$$\mathcal{M}(\alpha) = \left\{ X = \begin{pmatrix} U & V \\ L & W \end{pmatrix} \in \mathcal{M}_{ij}^k \middle| \operatorname{rank} W = \alpha \right\}.$$

于是形如 (2.8) 的 (P, Q) 必将 $\mathcal{M}(\alpha)$ 映到 $\mathcal{M}(\alpha)$. 所有这些 $\mathcal{M}(\alpha)$ 构成 $\mathcal{M}_{ij}^k$ 的一个分划. 因此有

$$|\mathcal{M}_{ij}^k| = \sum_{\alpha} |\mathcal{M}(\alpha)|, \tag{2.9}$$

这里 $0 \leqslant \alpha \leqslant \min(i, m-k)$, 后面将要看到 α 进一步满足的条件.

设 $\mathcal{M}(\alpha) \neq \varnothing$, 取定一个 $X \in \mathcal{M}(\alpha)$, 写 X 如形状 (2.7), 其中 $\operatorname{rank} W = \alpha$, 那么存在 $D \in GL_{m-k}(\mathbb{F}_q)$, $Z \in GL_{n-k}(\mathbb{F}_q)$ 使得

$$DWZ = \begin{array}{c} \begin{pmatrix} I^{(\alpha)} & 0 \\ 0 & 0 \end{pmatrix} \begin{array}{l} \alpha \\ m-k-\alpha \end{array} \\ \begin{array}{cc} \alpha & \quad n-k-\alpha \end{array} \end{array}.$$

如下选取

$$P = [I^{(k)}, D], \; Q = [I^{(k)}, Z],$$

那么 (P, Q) 使 X_1 和 X_2 均不动, 而将 X 化为

$$\begin{array}{c} \begin{pmatrix} U & V_1 & V_2 \\ L_1 & I^{(\alpha)} & 0 \\ L_2 & 0 & 0 \end{pmatrix} \begin{array}{l} k \\ \alpha \\ m-k-\alpha \end{array} \\ \begin{array}{ccc} k & \quad \alpha & \quad n-k-\alpha \end{array} \end{array}. \tag{2.10}$$

令 $\mathcal{M}_1$ 表示 $\mathcal{M}(\alpha)$ 中形如 (2.10) 的全体矩阵所成的集合, 于是

$$|\mathcal{M}_\alpha| = n_\alpha((m-k) \times (n-k), q)|\mathcal{M}_1|. \tag{2.11}$$

进一步对形如 (2.10) 的矩阵施行如下变换

$$\begin{pmatrix} I^{(k)} & -V_1 & \\ & I^{(\alpha)} & \\ & & I^{(m-k-\alpha)} \end{pmatrix} \begin{pmatrix} U & V_1 & V_2 \\ L_1 & I^{(\alpha)} & 0 \\ L_2 & 0 & 0 \end{pmatrix} \begin{pmatrix} I^{(k)} & & \\ -L_1 & I^{(\alpha)} & \\ & & I^{(n-k-\alpha)} \end{pmatrix}$$

$$= \begin{pmatrix} U^* & 0 & V_2 \\ 0 & I^{(\alpha)} & 0 \\ L_2 & 0 & 0 \end{pmatrix}.$$

令 $\mathcal{M}_2$ 为 $\mathcal{M}_1$ 中全体形如

$$\begin{array}{c}\begin{pmatrix} U & 0 & V \\ 0 & I^{(\alpha)} & 0 \\ L & 0 & 0 \end{pmatrix} \\ \begin{matrix} k \quad & \quad \alpha \quad & \quad n-k-\alpha \end{matrix}\end{array} \begin{matrix} k \\ \alpha \\ m-k-\alpha \end{matrix} \tag{2.12}$$

的矩阵所成的集合, 那么就有

$$|\mathcal{M}_1| = q^{2k\alpha}|\mathcal{M}_2|. \tag{2.13}$$

注意到如下的 (P, Q)

$$P = [A,\ I^{(\alpha)},\ D],\ Q = [A^{-1},\ I^{(\alpha)},\ Z],$$

这里 $A \in GL_k(\mathbb{F}_q)$, $D \in GL_{m-k-\alpha}$, $Z \in GL_{n-k-\alpha}$, 将形如 (2.12) 的矩阵变为

$$\begin{pmatrix} AUA^{-1} & O & AVZ \\ 0 & I^{(\alpha)} & 0 \\ DLA^{-1} & 0 & 0 \end{pmatrix},$$

因而将 $\mathcal{M}_2$ 变为 $\mathcal{M}_2$, 并且保持 V 和 L 的秩不变. 令 $\mathcal{M}_\beta$ 表示 $\mathcal{M}_2$ 中 $\operatorname{rank} L = \beta$ 的全体矩阵, 这里 $0 \leqslant \beta \leqslant \min(m-k-\alpha,\ k)$, $\alpha + \beta \leqslant i$. 于是

$$|\mathcal{M}_2| = \sum_\beta |\mathcal{M}_\beta|. \tag{2.14}$$

β 进一步满足的条件后面给出.

令 $\mathcal{M}_3$ 是 $\mathcal{M}_\beta$ 中全体形如

$$\begin{array}{c}\begin{pmatrix} U_1 & U_2 & 0 & V \\ 0 & 0 & I^{(\alpha)} & 0 \\ I^{(\beta)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \\ \begin{matrix} \beta \quad & \quad k-\beta \quad & \quad \alpha \quad & \quad n-k-\alpha \end{matrix}\end{array} \begin{matrix} k \\ \alpha \\ \beta \\ m-k-\alpha-\beta \end{matrix} \tag{2.15}$$

的矩阵所成的集合, 那么我们有

$$|\mathcal{M}_\beta| = n_\beta((m-k-\alpha) \times k, q)|\mathcal{M}_3|. \tag{2.16}$$

易见适当选取 (P, Q) 使 $\mathcal{M}_3$ 不变而将矩阵 (2.15) 中的 U_1 化为 0. 令 $\mathcal{M}_4$ 是 $\mathcal{M}_3$ 中全体形如

$$\begin{array}{c}\begin{pmatrix} 0 & U_2 & 0 & V \\ 0 & 0 & I^{(\alpha)} & 0 \\ I^{(\beta)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \\ \begin{matrix} \beta \quad & \quad k-\beta \quad & \quad \alpha \quad & \quad n-k-\alpha \end{matrix}\end{array} \begin{matrix} k \\ \alpha \\ \beta \\ m-k-\alpha-\beta \end{matrix} \tag{2.17}$$

的矩阵所成的集合, 那么我们有

$$|\mathcal{M}_3| = q^{\beta k}|\mathcal{M}_4|. \tag{2.18}$$

对于 $\mathcal{M}_4$ 中每个形如 (2.17) 的 $m\times n$ 矩阵, 作相应于块 U 和 V 的 $k\times(n-\alpha-\beta)$ 矩阵

$$Y = \begin{pmatrix} U & V \end{pmatrix} \begin{matrix} k \end{matrix},$$
$$\quad\ \begin{matrix} k-\beta & n-k-\alpha \end{matrix}$$

那么应有 $\operatorname{rank} Y = i-\alpha-\beta$. 再令 Y_1 为 $k\times(n-\alpha-\beta)$ 零矩阵, Y_2 为从 X_2 中取 (2.17) 中 U 和 V 对应位置上的元素构成的 $k\times(n-\alpha-\beta)$ 矩阵, 即

$$Y_2 = \begin{pmatrix} 0 & 0 \\ I^{(k-\beta)} & 0 \end{pmatrix} \begin{matrix} \beta \\ k-\beta \end{matrix}.$$
$$\quad\ \begin{matrix} k-\beta & n-k-\alpha \end{matrix}$$

于是 $\operatorname{rank} Y_2 = k-\beta$, $\operatorname{rank}(Y-Y_2) = j-\alpha-\beta$. 由此可知 $\alpha+\beta \leqslant j$. 令

$$\mathcal{M} = \{Y \in M_{k(n-\alpha-\beta)} | \operatorname{rank} Y = i-\alpha-\beta,\ \operatorname{rank}(Y-Y_2) = j-\alpha-\beta\},$$

那么

$$|\mathcal{M}_4| = |\mathcal{M}| = p^{k-\beta}_{i-\alpha-\beta,\, j-\alpha-\beta}(k\times(n-\alpha-\beta)). \tag{2.19}$$

这样, 我们从 (2.9), (2.11), (2.13), (2.14), (2.16), (2.18) 和 (2.19) 就得到下面的递推计算公式.

定理 2.9 设 $0<k<m$ 而 $m\leqslant n$, 我们有

$$p_{ij}^k(m\times n) = \sum_{\substack{0\leqslant\alpha\leqslant\min\{i,m-k\} \\ 0\leqslant\beta\leqslant\min\{k,m-k-\alpha\} \\ \alpha+\beta\leqslant\min\{i,j\}}} q^{k(2\alpha+\beta)} n_\alpha((m-k)\times(n-k),q)$$
$$\cdot n_\beta(k\times(m-k-\alpha),q)\cdot p^{k-\beta}_{i-\alpha-\beta,j-\alpha-\beta}(k\times(n-\alpha-\beta)),$$

这里如果 $m-\alpha-\beta=0$, 那么约定 $p^{k-\beta}_{i-\alpha-\beta,j-\alpha-\beta}(k\times 0)=1$.

如果 $k=m\leqslant n$, 而 i, j 中有小于 m 的, 比方说 $i<m$, 这时我们可以利用命题 1.1 中 (vi) 式来计算: $p_{ij}^m = \frac{k_i}{k_m}p_{mj}^i$. 不过当 $k=m$ 而 $m<n$ 时, 类似地我们有下面的计算公式.

定理 2.10 设 $k=m$ 而 $m<n$, 我们有

$$p_{ij}^m(m\times n) = \sum_{0\leqslant\beta\leqslant\min\{i,j,n-m\}} q^{m\beta}\ n_\beta(m\times(n-m),q)$$
$$\cdot p^{m-\beta}_{i-\beta,j-\beta}((m-\beta)\times m).$$

证明 略 □

如果 $k=m$ 并且 $m=n$, 计算 $P^m_{mm}(m\times m)$ 时, 上述两个公式均不能应用. 这时, 我们可以利用命题 1.1 中的 (v) 来如下计算

$$p^m_{mm}(m\times m)=k_m-\sum_{j=0}^{m-1}p^m_{mj}(m\times m).$$

下面我们给出关于 $p^m_{mm}(m\times m)$ 的一个递归算法. 为了书写简单, 将 $p^k_{ij}(m\times m)$ 记作 $p^k_{ij}(m)$.

定理 2.11 设 m 为一个正整数. 我们有

$$\begin{aligned}p^m_{mm}(m)= &\ q^{m-1}(q^m-q^{m-1}-1)p^{m-1}_{m-1m-1}(m-1)\\ &+q^{m-1}(q^{m-1}-1)p^{m-2}_{m-1m-1}(m-1).\end{aligned}$$

证明 取定 m 阶矩阵 $X_1=0$ 和 $X_2=I^{(m)}$. 令

$$\mathcal{M}=\{X\in M_{mm}|\mathrm{rank}\,X=m,\,\mathrm{rank}\,(X-X_2)=m\}.$$

那么 $p^m_{mm}(m)=|\mathcal{M}|$. 对于任意 $X\in\mathcal{M}$, 写

$$X=\begin{pmatrix}x_{11}&\cdots&x_{1m-1}&x_{1m}\\ \vdots&&\vdots&\vdots\\ x_{m-11}&\cdots&x_{m-1\,m-1}&x_{m-1m}\\ x_{m1}&\cdots&x_{m\,m-1}&x_{mm}\end{pmatrix}.$$

令 $\mathcal{M}_1$ 为 $\mathcal{M}$ 中全体形如

$$\begin{pmatrix}x_{11}&\cdots&x_{1m-1}&0\\ \vdots&&\vdots&\vdots\\ x_{m-1\,1}&\cdots&x_{m-1\,m-1}&0\\ x_{m1}&\cdots&x_{m\,m-1}&x_{mm}\end{pmatrix}\tag{2.20}$$

的矩阵作成的集合, 那么 $x_{mm}\neq 0,1$. 记 (2.20) 的左上角 $m-1$ 阶子矩阵为 $\widetilde{X}$, 那么 $\mathrm{rank}\,\widetilde{X}=m-1$. 并且 $\mathrm{rank}\,(\widetilde{X}-I^{(m-1)})=m-1$. 注意到 $x_{m1},\cdots,x_{m\,m-1}$ 的选取对形如 (2.20) 的矩阵之秩没有影响, 于是可得

$$|\mathcal{M}_1|=q^{m-1}(q-2)p^{m-1}_{m-1\,m-1}(m-1).\tag{2.21}$$

令 $\mathcal{M}_2=\mathcal{M}\backslash\mathcal{M}_1$, 那么

$$|\mathcal{M}|=|\mathcal{M}_1|+|\mathcal{M}_2|.$$

任取 $\mathcal{M}_2$ 中的一个元素 X, 其元素 $x_{1m}, \cdots, x_{m-1m}$ 不全为 0, 那么存在 $A \in GL_{m-1}(\mathbb{F}_q)$ 使得

$$A \begin{pmatrix} x_{1m} \\ x_{2m} \\ \vdots \\ x_{m-1m} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

令

$$P = [A, 1],$$

那么变换 $Y \mapsto PYP^{-1}$ 使 0 和 $I^{(m)}$ 不动, 并且使 $\mathcal{M}_2$ 不变, 而将元素 X 变为

$$Z = \begin{pmatrix} x'_{11} & \cdots & x'_{1\,m-2} & x'_{1\,m-1} & 0 \\ \vdots & & \vdots & \vdots & \vdots \\ x'_{m-2\,1} & \cdots & x'_{m-2\,m-2} & x'_{m-2\,m-1} & 0 \\ x'_{m-1\,1} & \cdots & x'_{m-1\,m-2} & x'_{m-1\,m-1} & 1 \\ x'_{m1} & \cdots & x'_{m\,m-2} & x'_{m\,m-1} & x_{mm} \end{pmatrix}. \tag{2.22}$$

令 $\mathcal{M}_3$ 是 $\mathcal{M}_2$ 中全体形如 (2.22) 的矩阵作成的集合, 那么有

$$|\mathcal{M}_2| = (q^{m-1} - 1)|\mathcal{M}_3|. \tag{2.23}$$

将形如 (2.22) 的矩阵的右下角元素化为 0, 即将它的第 $m-1$ 行乘以 $-x_{mm}$ 后加到第 m 行上, 得

$$\begin{pmatrix} x'_{11} & \cdots & x'_{1\,m-2} & x'_{1\,m-1} & 0 \\ \vdots & & \vdots & \vdots & \vdots \\ x'_{m-2\,1} & \cdots & x'_{m-2\,m-2} & x'_{m-2\,m-1} & 0 \\ x'_{m-1\,1} & \cdots & x'_{m-1\,m-2} & x'_{m-1\,m-1} & 1 \\ y_1 & \cdots & y_{m-2} & y_{m-1} & 0 \end{pmatrix},$$

这里

$$y_i = x'_{mi} - x'_{m-1\,i}x_{mm},\ i = 1, \cdots, m-1.$$

我们看出这个矩阵的第 $m-1$ 行上的元素 $x'_{m-1\,1}, \cdots, x'_{m-1\,m-1}$ 之取值, 对于它的秩没有影响. 划去它的第 $m-1$ 行和第 m 列, 得

$$\widetilde{Z} = \begin{pmatrix} x'_{11} & \cdots & x'_{1\,m-2} & x'_{1\,m-1} \\ \vdots & & \vdots & \vdots \\ x'_{m-2\,1} & \cdots & x'_{m-2\,m-2} & x'_{m-2\,m-1} \\ y_1 & \cdots & y_{m-2} & y_{m-1} \end{pmatrix}, \tag{2.24}$$

那么, $\operatorname{rank}\widetilde{Z} = m-1$. 现在对 $Z - I^{(m)}$ 施行类似变换, 将它的右下角元素化为 0, 即将它的第 $m-1$ 行乘以 $-(x_{mm}-1)$ 后加到第 m 行上, 我们得到

$$\begin{pmatrix} x'_{11}-1 & \cdots & x'_{1\,m-2} & x'_{1\,m-1} & 0 \\ \vdots & & \vdots & \vdots & \vdots \\ x'_{m-2\,1} & \cdots & x'_{m-2\,m-2}-1 & x'_{m-2\,m-1} & 0 \\ x'_{m-1\,1} & \cdots & x'_{m-1\,m-2} & x'_{m-1\,m-1}-1 & 1 \\ y_1+x'_{m-1\,1} & \cdots & y_{m-2}+x'_{m-1\,m-2} & y_{m-1}+x'_{m-1\,m-1}+x_{mm}-1 & 0 \end{pmatrix},$$

这个矩阵的秩为 m. 因此, 划去它的第 $m-1$ 行和第 m 列, 我们得到 $m-1$ 阶矩阵

$$\begin{pmatrix} x'_{11}-1 & \cdots & x'_{1\,m-2} & x'_{1\,m-1} \\ \vdots & & \vdots & \vdots \\ x'_{m-2\,1} & \cdots & x'_{m-2\,m-2}-1 & x'_{m-2\,m-1} \\ y_1+x'_{m-1\,1} & \cdots & y_{m-2}+x'_{m-1\,m-2} & y_{m-1}+x'_{m-1\,m-1}+x_{mm}-1 \end{pmatrix},$$

它的秩为 $m-1$. 现在令

$$\widetilde{Z}_2 = \begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & & 1 & \cdots & 0 \\ -x'_{m-1\,1} & \cdots & -x'_{m-1\,m-2} & & 1-x'_{m-1\,m-1}-x_{mm} \end{pmatrix},$$

那么 $\operatorname{rank}(\widetilde{Z}-\widetilde{Z_2}) = m-1$, 而

$$\operatorname{rank}\widetilde{Z_2} = \begin{cases} m-2, & \text{如果 } x'_{m-1\,m-1}+x_{mm}=1, \\ m-1, & \text{如果 } x'_{m-1\,m-1}+x_{mm}\neq 1. \end{cases}$$

令 $\mathcal{M}_{31}$ 是 $\mathcal{M}_3$ 中对于取定 $x'_{m-1\,1},\cdots,x'_{m-1\,m-1}$ 后, 而取 $x_{mm}\neq 1-x'_{m-1\,m-1}$ 的那些矩阵作成的集合, 相应地得到 (2.24) 中矩阵的集合记作 $\widetilde{\mathcal{M}}_{31}$, 那么有

$$|\mathcal{M}_{31}| = q^{m-1}(q-1)|\widetilde{\mathcal{M}}_{31}|,\ |\widetilde{\mathcal{M}}_{31}| = p^{m-1}_{m-1\,m-1}(m-1). \tag{2.25}$$

同理, 令 $\mathcal{M}_{32}$ 是 $\mathcal{M}_3$ 中对于取定 $x'_{m-1\,1},\cdots,x'_{m-1\,m-1}$ 后而取 $x_{mm}=1-x'_{m-1\,m-1}$ 的那些矩阵作成的集合, 相应地得到 (2.24) 中矩阵的集合记作 $\widetilde{\mathcal{M}}_{32}$, 那么有

$$|\mathcal{M}_{32}| = q^{m-1}|\widetilde{\mathcal{M}}_{32}|,\ |\widetilde{\mathcal{M}}_{32}| = p^{m-2}_{m-1\,m-1}(m-1). \tag{2.26}$$

由 (2.21), (2.23), (2.25) 和 (2.26) 即得本定理中的公式. □

§2.4 长方阵结合方案的自对偶性

在这一节中, 我们要证明结合方案 $\mathrm{Mat}(m \times n, q)$ 是自对偶的.

设 $m \leqslant n$, 结合方案 $\mathrm{Mat}(m \times n, q)$ 的类数为 m, 结合关系

$$R_i = \{(X, Y) | Y - X \in C_i\}, i = 0, 1, \cdots, m,$$

这里 C_i 为 $\mathbb{F}_q$ 上全体秩为 i 的 $m \times n$ 的矩阵的集合. M_{mn} 对于矩阵加法作成一个交换群, 它的特征标群记作 M_{mn}^*.

现在, 任意取定基域的加法群 $(\mathbb{F}_q, +)$ 在复数域 $\mathbb{C}$ 上的一个非平凡不可约特征标 χ. 对于每个矩阵 $A = (a_{ij}) \in M_{mn}$, 我们定义映射

$$\begin{aligned} \phi_A : M_{mn} &\longrightarrow \mathbb{C} \\ X = (x_{ij}) &\longmapsto \chi\left(\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}x_{ij}\right). \end{aligned} \tag{2.27}$$

容易看出, ϕ_A 是 M_{mn} 的一个特征标, 并且有

$$\phi_{A+B} = \phi_A \phi_B. \tag{2.28}$$

命题 2.12 设 $A, B \in M_{mn}$, 那么 $\phi_A = \phi_B$ 当且仅当 $A = B$. 于是映射 $A \mapsto \phi_A$ 是 M_{mn} 到 M_{mn}^* 的一个同构.

证明 先证命题的前一个论断. 充分性是显然的, 往证必要性. 设 $A = (a_{ij}), B = (b_{ij})$ 而有

$$\phi_A(X) = \phi_B(X), \ \forall X = (x_{ij}) \in M_{mn},$$

即

$$\chi\left(\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}x_{ij}\right) = \chi\left(\sum_{i=1}^{m}\sum_{j=1}^{n} b_{ij}x_{ij}\right) \quad \forall x_{ij} \in \mathbb{F}_q.$$

对于 i, j, 取 $x_{kl} = 0, k \neq i, l \neq j$, 就有 $\chi(a_{ij}x_{ij}) = \chi(b_{ij}x_{ij}) \ \forall x_{ij} \in \mathbb{F}_q$. 于是

$$\chi((a_{ij} - b_{ij})x_{ij}) = 1, \ \forall x_{ij} \in \mathbb{F}_q.$$

因为 χ 是非平凡特征标, 我们立得 $a_{ij} = b_{ij}\ (i = 1, \cdots, m;\ j = 1, \cdots, n)$, 即 $A = B$.

命题的后一论断从 $|M_{mn}| = |M_{mn}^*|$ 和 (2.28) 可得. □

命题 2.13 对于 $A, X \in M_{mn}$, $P \in GL_m(\mathbb{F}_q)$, $Q \in GL_n(\mathbb{F}_q)$ 恒有

$$\phi_A(PXQ) = \phi_{{}^tPA{}^tQ}(X).$$

证明　设 $A=(a_{ij})$, $X=(x_{ij})$, $P=(p_{ij})$, $Q=(q_{ij})$. 再记 $PXQ=(x_{ij}^*)$, 这里 $x_{ij}^*=\sum_{k=1}^{m}\sum_{l=1}^{n}p_{ik}x_{kl}q_{lj}$, 依定义有

$$\begin{aligned}\phi_A(PXQ)&=\chi\left(\sum_{i=1}^{m}\sum_{j=1}^{n}a_{ij}x_{ij}^*\right)\\&=\chi\left(\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{m}\sum_{l=1}^{n}a_{ij}p_{ik}x_{kl}q_{lj}\right)\\&=\chi\left(\sum_{k=1}^{m}\sum_{l=1}^{n}\left(\sum_{i=1}^{m}\sum_{j=1}^{n}p_{ik}a_{ij}q_{lj}\right)x_{kl}\right)\\&=\phi_{{}^tPA{}^tQ}(X).\end{aligned}$$

□

设 $\mathbb{C}_i$ 表示等价类 C_i 在 M_{mn} 的群代数 $\mathbb{C}[M_{mn}]$ 中的形式和, $\mathfrak{S}$ 是由 $\mathbb{C}_0, \mathbb{C}_1, \cdots, \mathbb{C}_m$ 生成的 S 环, 由 $\mathfrak{S}$ 确定的结合方案 $\mathfrak{X}(\mathfrak{S})$ 就是 $\mathrm{Mat}(m\times n, q)$. 对于 $i\in\{0, 1, \cdots, m\}$, 令

$$\phi_A(\mathbb{C}_i)=\sum_{X\in C_i}\phi_A(X). \tag{2.29}$$

由定理 1.16 知, ϕ_A 是结合关系 R_i 的邻接矩阵 A_i 的属于特征值 $\phi_A(\mathbb{C}_i)$ 的特征向量. 设 $A, B\in M_{mn}$, 并且 $\mathrm{rank}\,A=\mathrm{rank}\,B$, 那么存在 $P\in GL_m(\mathbb{F}_q)$ 和 $Q\in GL_n(\mathbb{F}_q)$ 使得 $B=PAQ$. 由命题 2.13 可推得

$$\phi_B(\mathbb{C}_i)=\phi_{PAQ}(\mathbb{C}_i)=\phi_A(\mathbb{C}_i),\ i=0, 1, \cdots, m. \tag{2.30}$$

由定理 1.14, 在 M_{mn}^* 中确定了等价类 $Y_0, Y_1, \cdots, Y_m$, 这里

$$Y_j=\{\phi_A|A\in C_j\},\ j=0, 1, \cdots, m.$$

从而确定了 M_{mn}^* 上的一个 S 环 $\mathfrak{S}^*$. 由 $\mathfrak{S}^*$ 确定的结合方案 $\mathfrak{X}(\mathfrak{S}^*)$ 和 $\mathrm{Mat}(m\times n, q)$ 是形式对偶的. 现在, 映射 $A\to\phi_A$ 是 M_{mn} 和 M_{mn}^* 之间的一个同构. 在此同构映射下, 给出结合方案 $\mathrm{Mat}(m\times n, q)$ 和 $\mathfrak{X}(\mathfrak{S}^*)$ 的一个同构. 因此, 它们有相同的交叉数, 于是我们有

定理 2.14　长方阵结合方案 $\mathrm{Mat}(m\times n, q)$ 是自对偶的.

对于定理 2.14, 我们给出如下一个直接证明. 从 (2.29), (2.30) 和定理 1.16 可知, 结合方案 $\mathrm{Mat}(m\times n, q)$ 的第一特征值矩阵 $P=(p_i(j))$ 的 (j, i) 位置元素为

$$p_i(j)=\phi_A(\mathbb{C}_i)=\sum_{X\in C_i}\phi_A(X),\ A\in C_j.$$

依定义 (2.27) 可知, $\phi_A(X)=\phi_X(A)$, 于是通过计算 $\sum_{A\in C_j}\sum_{X\in C_i}\phi_A(X)$ 可得

$$k_j p_i(j) = k_i p_j(i).$$

利用这个关系式, 我们可以得到

$$P^2 = |M_{mn}|I.$$

实际上

$$\begin{aligned}\sum_{l=0}^{m} p_l(i)p_j(l) &= \sum_{l=0}^{m} p_i(l)p_j(l)k_l/k_i \\ &= \frac{1}{k_i}\sum_{X\in C_i}\sum_{Y\in C_j}\sum_{A\in M_{mn}}\phi_A(X)\phi_A(Y) \\ &= \frac{1}{k_i}\sum_{X\in C_i}\sum_{Y\in C_j}\left(\sum_{A\in M_{mn}}\phi_A(X+Y)\right) \\ &= |M_{mn}|\delta_{ij}.\end{aligned}$$

这里用到特征标的一个性质: 当 $X+Y\neq 0$ 时, $\sum_{A\in M_{mn}}\phi_A(X+Y)=0$, 及 X 和 $-X$ 在同一个类中.

由定理 2.7 和定理 2.14 立得

定理 2.15 长方阵结合方案 $\mathrm{Mat}(m\times n,\,q)$ 是 (P 和 Q) 多项式的.

§2.5 长方阵结合方案的自同构

关于长方阵结合方案的自同构, 我们有下面的

定理 2.16 设 $1<m\leqslant n$. 长方阵结合方案 $\mathrm{Mat}(m\times n,\,q)$ 的每个自同构必为下列形状

$$X \longmapsto PX^{\sigma}Q + A,\ \forall X\in M_{mn}, \tag{2.31}$$

这里 $P\in GL_m(\mathbb{F}_q)$, $Q\in GL_n(\mathbb{F}_q)$, $A\in M_{mn}$, σ 是 $\mathbb{F}_q$ 的一个自同构.

如果 $m=n$, 那么除了 (2.31) 形状之外, 还有

$$X \longmapsto P({}^tX)^{\sigma}Q + A,\ \forall X\in M_{mm}, \tag{2.32}$$

这里 ${}^tX$ 表示 X 的转置.

证明　设 $q=p^t$. 由定理 2.1 知, 结合方案 $\mathrm{Mat}(m\times n,\,q)$ 的价 k_i 中所含素数 p 的因子为 $p^{\frac{1}{2}i(i-1)t}$. 所以它的价 $k_1,\,k_2,\,\cdots,\,k_m$ 两两不等. 于是由推论 1.28(i), $\mathrm{Mat}(m\times n,\,q)$ 的每个自同构均为内自同构.

又由定理 2.7, 结合方案 $\mathrm{Mat}(m\times n,\,q)$ 关于顺序 $R_0,\,R_1,\,\cdots,\,R_m$ 是 P 多项式的, 于是由推论 1.28(ii) 知,$\mathrm{Mat}(m\times n,\,q)$ 的每个自同构均为关系 R_1 的图 $\Gamma^{(1)}$ 的自同构.

进而, 由长方阵仿射几何基本定理 [16] 知, 图 $\Gamma^{(1)}$ 的自同构必为形状 (2.31) 或 (2.32). 于是本定理得证. □

注意, 当 $m=1$ 时 $\mathrm{Mat}(1\times n,\,q)$ 是平凡的. 而它的图 $\Gamma^{(1)}$ 是一个 q^n 个顶点的完全图 (即它的任意两个不同顶点都邻接), 记作 K_{q^n}.

第三章　交错矩阵的结合方案

§3.1　交错矩阵结合方案的本原性和 P 多项式性质

令 $\mathbb{F}_q$ 为 q 元有限域, $n \geqslant 2$ 是一个整数. $\mathbb{F}_q$ 上的 $n \times n$ 矩阵 $A=(a_{ij})$ 叫做**交错的**, 如果对于 $i \neq j$ 有 $a_{ij}+a_{ji}=0$, 并且 $a_{ii}=0\,(1 \leqslant i,j \leqslant n)$. 令 $\mathcal{K}(n,\,q)$ 表示 $\mathbb{F}_q$ 上全体 $n \times n$ 交错矩阵的集合. 显然 $\mathcal{K}(n,\,q)$ 对于矩阵加法及 $\mathbb{F}_q$ 中元素对于矩阵的纯量乘法都是封闭的, 因而 $\mathcal{K}(n,\,q)$ 是 $\mathbb{F}_q$ 上全体 $n \times n$ 矩阵所成的向量空间 $M_n(q)$ 的一个子空间. 注意到

$$\{E_{ij}-E_{ji} | 1 \leqslant i < j \leqslant n\}$$

作成 $\mathcal{K}(n,\,q)$ 的一个基, 所以 $\dim \mathcal{K}(n,\,q)=\frac{1}{2}n(n-1)$.

对于 $\mathbb{F}_q$ 上任一 $n \times n$ 可逆矩阵 T 及任一 $n \times n$ 交错矩阵 X 我们恒有 $TX\,{}^tT$ 仍为 $n \times n$ 交错矩阵, 于是 $GL_n(\mathbb{F}_q)$ 可以如下自然地作用在 $\mathcal{K}(n,\,q)$ 上

$$\begin{array}{rcl}\mathcal{K}(n,\,q)\times GL_n(\mathbb{F}_q) & \longrightarrow & \mathcal{K}(n,\,q) \\ (X,\quad T) & \longmapsto & TX\,{}^tT,\end{array} \tag{3.1}$$

这里 ${}^tT$ 表示矩阵 T 的转置. 易见, 每个 $T \in GL_n(\mathbb{F}_q)$ 都给出加法群 $\mathcal{K}(n,\,q)$ 的一个自同构. 进一步知, 这个作用给出群 $GL_n(\mathbb{F}_q)$ 在 $\mathcal{K}(n,\,q)$ 上的一个线性表示, 其核为 $\{\pm I^{(n)}\}$.

令 T_0 表示加法群 $\mathcal{K}(n,\,q)$ 的平移群, 再设 G 是由 $GL_n(\mathbb{F}_q)$ 和 T_0 生成的群. G 是 $\mathcal{K}(n,\,q)$ 上的一个置换群, 并且可迁地作用在 $\mathcal{K}(n,\,q)$ 上. 于是由定理 1.4, $(G,\,\mathcal{K}(n,\,q))$ 决定 $\mathcal{K}(n,\,q)$ 上的一个交换结合方案, 叫做 **$\mathbb{F}_q$ 上 n 阶交错矩阵的结合方案**, 记作 $\mathrm{Alt}(n,\,q)$.

显然, $|\mathcal{K}(n,\,q)|=q^{\frac{1}{2}n(n-1)}$. 由定理 1.4 可知, 这个结合方案的类数等于 $GL_n(\mathbb{F}_q)$ 在 $\mathcal{K}(n,\,q)$ 上的非平凡轨道数. $\mathcal{K}(n,\,q)$ 中的两个元素 X 和 Y 在同一个 $GL_n(\mathbb{F}_q)$ 轨道, 当且仅当存在矩阵 $T \in GL_n(\mathbb{F}_q)$ 使得 $Y=TX\,{}^tT$, 即 X 与 Y 合同.

从线性代数知 (可参看 [15]), 每个交错矩阵的秩均为偶数. 设 $X \in \mathcal{K}(n,\,q)$, $\mathrm{rank}\,X=2i\,(0 \leqslant 2i \leqslant n)$, 那么存在 $T \in GL_n(\mathbb{F}_q)$ 使得

$$TX\,{}^tT=\left[\begin{pmatrix}0 & 1\\-1 & 0\end{pmatrix},\cdots,\begin{pmatrix}0 & 1\\-1 & 0\end{pmatrix},0^{(n-2i)}\right]. \tag{3.2}$$

因而 $\mathcal{K}(n, q)$ 中两个矩阵 X 和 Y 在同一个 $GL_n(\mathbb{F}_q)$ 轨道, 当且仅当 $\operatorname{rank} X = \operatorname{rank} Y$. 于是结合方案 $\operatorname{Alt}(n, q)$ 的类数为 $[\frac{n}{2}]$. 令

$$C_i = \{X \in \mathcal{K}(n, q) | \operatorname{rank} X = 2i\},\ 0 \leqslant i \leqslant \left[\frac{n}{2}\right]. \tag{3.3}$$

那么, 对应的结合类为

$$R_i = \{(X, Y) | Y - X \in C_i\},\ 0 \leqslant i \leqslant \left[\frac{n}{2}\right]. \tag{3.4}$$

易见, 每个 R_i 都是对称的, 因而结合方案 $\operatorname{Alt}(n, q)$ 是对称的.

下面, 我们讨论这个结合方案的本原性. 类似于定理 2.2, 我们有

定理 3.1　群 $GL_n(\mathbb{F}_q)$ 在 $\mathcal{K}(n, q)$ 上的表示 (3.1) 是不可约的.

证明　设 W 是 $\mathcal{K}(n, q)$ 的一个 $GL_n(\mathbb{F}_q)$ 不变子空间, 并且 $W \neq 0$. 任取 W 中的一个矩阵 $A \neq 0$. 设 $\operatorname{rank} A = 2i > 0$. 由于 W 是 $GL_n(\mathbb{F}_q)$ 不变的, 对于任意 $T \in GL_n(\mathbb{F}_q)$ 均有 $TA\,{}^tT \in W$, 于是 W 包有 $\mathcal{K}(n, q)$ 中全体秩为 $2i$ 的交错矩阵. 如果 $i = 1$, 那么 W 包有 $\mathcal{K}(n, q)$ 中全体秩为 2 的交错矩阵. 由 (3.2) 可知, 每个非零交错矩阵均可表示成若干个秩为 2 的交错矩阵之和. 于是 $\mathcal{K}(n, q)$ 中每个矩阵均在 W 之中, 即 $W = \mathcal{K}(n, q)$.

现在设 $i \geqslant 2$, 因而 $n \geqslant 4$. W 包有如下两个秩为 $2i$ 的交错矩阵

$$A_1 = \left[\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \cdots, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, 0^{(n-2i)}\right],$$

$$A_2 = \left[\begin{pmatrix} 0 & 1 & 1 & 0 \\ -1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \cdots, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, 0^{(n-2i)}\right].$$

于是 W 包有 $A_1 - A_2$, 而 $\operatorname{rank}(A_1 - A_2) = 2$. 这就归结到 $i = 1$ 的情形. □

定理 3.2　群 $G = GL_n(\mathbb{F}_q) \cdot T_0$(半直积) 作用在 $\mathcal{K}(n, q)$ 上是本原的.

证明　G 的元素表示成 (T, A) $(T \in GL_n(\mathbb{F}_q),\ A \in \mathcal{K}(n, q))$, 它在 $\mathcal{K}(n, q)$ 上的作用为

$$(T, A) : X \longmapsto TX\,{}^tT + A,\ \forall X \in \mathcal{K}(n, q). \tag{3.5}$$

G 中两个元素 (T_1, A_1) 和 (T_2, A_2) 的乘积为

$$(T_1, A_1)(T_2, A_2) = (T_2T_1,\ T_2A_1\,{}^tT_2 + A_2). \tag{3.6}$$

类似于定理 2.3 的证明即可证明本定理, 故下略. □

由定理 3.2 和定理 1.18 我们就有

定理 3.3 设 $n \geqslant 2$. 交错矩阵结合方案 $\mathrm{Alt}(n, q)$ 是本原的.

令 $\Gamma^{(i)}\ (i \neq 0)$ 表示 $\mathrm{Alt}(n, q)$ 的结合关系 R_i 的关系图, 即 $\Gamma^{(i)}$ 以 $\mathcal{K}(n, q)$ 为其顶点集, 而以 R_i 为其边集. 由于 R_i 为对称的, 我们认为边 (X, Y) 与边 (Y, X) 重合, 即 $\Gamma^{(i)}$ 为无向图. 由定理 3.3 知, $\mathrm{Alt}(n, q)$ 的每个关系图 $\Gamma^{(i)}\ (i = 1, \cdots, [\frac{n}{2}])$ 都是连通的. 又由 (3.5) 可知, 群 G 的每个元素 (T, A) 将 $\Gamma^{(i)}$ 的边映到边, 因而 G 是 $\Gamma^{(i)}$ 的一个自同构群.

我们进一步考察图 $\Gamma^{(1)}$, 它以 $\mathbb{F}_q$ 上全体 n 阶交错矩阵为其顶点, 两顶点 X 与 Y 邻接, 如果 $\mathrm{rank}(Y - X) = 2$. 设 $X = X_0, X_1, \cdots, X_{s-1}, X_s = Y$ 是图 $\Gamma^{(1)}$ 从顶点 X 到顶点 Y 的一条长为 s 的道路, 即 $\mathrm{rank}(X_i - X_{i-1}) = 2$. 由线性代数知

$$\begin{aligned}2s &= \mathrm{rank}(X_1 - X_0) + \mathrm{rank}(X_2 - X_1) + \cdots \\ &\quad + \mathrm{rank}(X_s - X_{s-1}) \geqslant \mathrm{rank}(Y - X).\end{aligned}$$

特别地, X 到 Y 的距离 $\partial(X, Y) \geqslant \frac{1}{2}\mathrm{rank}(Y - X)$.

我们进一步证明上式中等号成立. 不失一般性, 可设 $X = 0$, $\mathrm{rank}\, Y = 2r > 0$. 由 (3.2) 可设

$$Y = \left[\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \cdots, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, 0^{(n-2r)}\right].$$

$$Y_i = \left[\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \cdots, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, 0^{(n-2i)}\right], i = 0, 1, \cdots, r.$$

那么 $\mathrm{rank}\,(Y_i - Y_{i-1}) = 2$, 所以 Y_{i-1} 与 Y_i 邻接, 于是 $Y_0 = X, Y_1, \cdots, Y_{r-1}, Y_r = Y$ 是 X 与 Y 之间的一条道路, 因而 $\partial(X, Y) \leqslant \frac{1}{2}\mathrm{rank}\,(Y - X)$. 这样, 我们就有

定理 3.4 对于结合方案 $\mathrm{Alt}(n, q)$ 的关系图 $\Gamma^{(1)}$, 恒有

$$\partial(X, Y) = \frac{1}{2}\mathrm{rank}\,(Y - X).$$

从上面的证明过程可知, 我们有下面的

定理 3.5 交错矩阵结合方案的关系图 $\Gamma^{(1)}$ 是距离可迁的, 因而是距离正则的.

由定理 3.5, $\Gamma^{(1)}$ 中距离为 i 的顶点对子 (X, Y) 恰好组成结合方案 $\mathrm{Alt}(n, q)$ 的结合关系 $R_i\ (i = 0, \cdots, [\frac{n}{2}])$. 因此, 由定理 1.24, 我们有

定理 3.6 设 $n \geqslant 2$. $\mathbb{F}_q$ 上的 n 阶交错矩阵的结合方案 $\mathrm{Alt}\ (n, q)$ 是 P 多项式的.

文献中把结合关系图 $\Gamma^{(1)}$ 叫做*交错矩阵的图*, 记作 $\mathrm{Alt}(n, q)$. 由于这个图完全决定了交错矩阵的结合方案, 我们也自然地把这个结合方案记作 $\mathrm{Alt}(n, q)$.

§3.2 关系图 $\Gamma^{(1)}$ 的参数

在这一节中, 我们计算结合方案 $\text{Alt}(n, q)$ 的关系图 $\Gamma^{(1)}$ 的参数. 为了计算上的方便, 我们将引用文献 [15] 中关于辛几何的两个计数公式. 为此, 我们先介绍有关的概念, 然后进行参数计算.

设 ν 为一正整数, $\mathbb{F}_q$ 为 q 元域, 取定 $2\nu \times 2\nu$ 交错矩阵

$$K_\nu = \begin{pmatrix} 0 & I^{(\nu)} \\ -I^{(\nu)} & 0 \end{pmatrix}.$$

$\mathbb{F}_q$ 上 $2\nu \times 2\nu$ 矩阵 T 叫做一个关于 K_ν 的辛矩阵, 如果 T 满足条件

$$TK_\nu {}^tT = K_\nu. \tag{3.7}$$

容易看出, 辛矩阵都是可逆的, 并且, $\mathbb{F}_q$ 上全体关于 K_ν 的辛矩阵对于矩阵乘法做成一个群, 叫做 $\mathbb{F}_q$ 上关于 K_ν 的 2ν 阶辛群, 记作 $Sp_{2\nu}(K_\nu, \mathbb{F}_q)$. 由 [15] 中定理 3.16 知, 辛群 $Sp_{2\nu}(K_\nu, \mathbb{F}_q)$ 的阶为

$$|Sp_{2\nu}(K_\nu, \mathbb{F}_q)| = q^{\nu^2}\prod_{j=1}^{\nu}(q^{2j}-1). \tag{3.8}$$

辛群 $Sp_{2\nu}(K_\nu, \mathbb{F}_q)$ 是 $GL_{2\nu}(\mathbb{F}_q)$ 的一个子群. 注意到 $K_\nu^2 = -I^{(2\nu)}$, 进一步可知

$$TK_\nu {}^tT = K_\nu \iff {}^tTK_\nu T = K_\nu.$$

就是说, $T \in Sp_{2\nu}(K_\nu, \mathbb{F}_q)$, 当且仅当 ${}^tT \in Sp_{2\nu}(K_\nu, \mathbb{F}_q)$.

令 $\mathbb{F}_q^{(2\nu)}$ 表示 $\mathbb{F}_q$ 上 2ν 维行向量空间. 辛群 $Sp_{2\nu}(K_\nu, \mathbb{F}_q)$ 如下自然地作用在 $\mathbb{F}_q^{(2\nu)}$ 上:

$$\begin{array}{ccc} \mathbb{F}_q^{(2\nu)} \times Sp_{2\nu}(K_\nu, \mathbb{F}_q) & \longrightarrow & \mathbb{F}_q^{(2\nu)} \\ ((x_1, \cdots, x_{2\nu}), T) & \longmapsto & (x_1, \cdots, x_{2\nu})T. \end{array} \tag{3.9}$$

向量空间 $\mathbb{F}_q^{(2\nu)}$ 连同辛群 $Sp_{2\nu}(K_\nu, \mathbb{F}_q)$ 的作用称为 (由 K_ν 决定的) 辛空间. 辛矩阵 T 在 $\mathbb{F}_q^{(2\nu)}$ 上的作用是线性的, 因而它自然地作用在 $\mathbb{F}_q^{(2\nu)}$ 的子空间的集合上.

设 P 是 $\mathbb{F}_q^{(2\nu)}$ 的一个 m 维子空间. 任取 P 的一个基 $v_1, \cdots, v_m$, 由它们作为行构作一个秩为 m 的 $m \times 2\nu$ 矩阵, 叫做子空间 P 的一个矩阵表示. 在下面的讨论中, 我们常常把这个矩阵仍记为 P. 矩阵 $PK_\nu {}^tP$ 是一个 $m \times m$ 交错矩阵, 因而它的秩为偶数, 设 $\text{rank}\, PK_\nu {}^tP = 2s$, 这里 s 满足条件 $2s \leqslant m \leqslant \nu + s$ ([15]). 由于 $PK_\nu {}^tP$ 的秩与子空间 P 的矩阵表示的选取无关, 我们称子空间 P 为 (m, s) 型子空间. 下面的 $m \times 2\nu$ 矩阵

$$\begin{array}{c} \left(\begin{array}{cccccc} I^{(s)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(s)} & 0 & 0 \\ 0 & I^{(m-2s)} & 0 & 0 & 0 & 0 \end{array}\right) \begin{array}{c} s \\ s \\ m-2s \end{array} \\ \begin{array}{cccccc} s & m-2s & \nu+s-m & s & m-2s & \nu+s-m \end{array} \end{array} \tag{3.10}$$

表示一个 (m, s) 型子空间.

在辛群 $Sp_{2\nu}(K_\nu, \mathbb{F}_q)$ 作用下, $\mathbb{F}_q^{(2\nu)}$ 中类型相同的子空间组成一个轨道. 令 $N(m, s; 2\nu)$ 表示 $\mathbb{F}_q^{(2\nu)}$ 中全体 (m, s) 型子空间的个数, 由 [15] 的定理 3.18 知

$$N(m, s; 2\nu) = q^{2s(\nu+s-m)} \frac{\prod\limits_{j=\nu+s-m+1}^{\nu} (q^{2j}-1)}{\prod\limits_{j=1}^{s}(q^{2j}-1) \prod\limits_{j=1}^{m-2s} (q^{j}-1)}. \tag{3.11}$$

在后面的计算中我们将用到下面关于矩阵的一个计数公式. 设 A 是 $\mathbb{F}_q$ 上的一个 $l \times 2\nu$ 矩阵. 如果 $\operatorname{rank} A = m$, 而 $\operatorname{rank} AK_\nu {}^tA = 2s$, 那么我们称 A 是关于 K_ν 的一个(m, s) 型矩阵, 这里 m, s, ν 仍满足条件 $2s \leqslant m \leqslant \nu + s$. 令 $n(l \times 2\nu; m, s)$ 表示 $\mathbb{F}_q$ 上全体关于 K_ν 为 (m, s) 型的 $l \times 2\nu$ 矩阵的个数. 我们有如下的

定理 3.7 设 $l \geqslant m$. $\mathbb{F}_q$ 上关于 K_ν 为 (m, s) 型的 $l \times 2\nu$ 矩阵个数

$$\begin{aligned} &n(l \times 2\nu; m, s) \\ &= q^{2s(\nu+s-m)+\frac{1}{2}m(m-1)} \frac{\prod\limits_{j=\nu+s-m+1}^{\nu} (q^{2j}-1) \prod\limits_{j=l-m+1}^{l} (q^{j}-1)}{\prod\limits_{j=1}^{s}(q^{2j}-1) \prod\limits_{j=1}^{m-2s} (q^{j}-1)}. \end{aligned} \tag{3.12}$$

证明 设 A 是一个关于 K_ν 为 (m, s) 型的 $l \times 2\nu$ 矩阵. 由 A 的 l 个行向量生成 $\mathbb{F}_q^{(2\nu)}$ 的一个子空间 P, 这个子空间的型就是 (m, s). 反之, 设 P 是 $\mathbb{F}_q^{(2\nu)}$ 的一个 (m, s) 型子空间, 任取 P 的一组由 l 个向量组成的生成元, 以这 l 个向量作为行构成的矩阵就是一个关于 K_ν 为 (m, s) 型的 $l \times 2\nu$ 矩阵.

现在, 对于每个 (m, s) 型子空间 P, 我们取定 P 的一个基 $v_1, \cdots, v_m$. 任取一个 $l \times m$ 矩阵 M 使得 $\operatorname{rank} M = m$, 那么

$$M \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix}$$

就是一个关于 K_ν 为 (m, s) 型的 $l \times 2\nu$ 矩阵. 易见不同的 M 得到不同的 $l \times 2\nu$ 矩阵. 由不同类型的子空间得到不同类型之 $l \times 2\nu$ 矩阵. 所以有

$$n(l \times 2\nu; m, s) = n_m(l \times m, q)N(m, s; 2\nu),$$

这里 $n_m(l \times m, q)$ 表示秩为 m 的 $l \times m$ 矩阵的个数. 由定理 2.1 中的公式和 (3.11) 立得 (3.12). □

现在, 回到我们的交错矩阵结合方案.Alt(n, q) 的结合关系 R_i 的价 $k_i = |C_i|$. 令 $K_i(n, q)$ 表示 $\mathbb{F}_q$ 上秩为 $2i$ 的 $n \times n$ 交错矩阵的个数, 即 $|C_i| = K_i(n, q)$. 我们有下面的

定理 3.8 设 $n \geqslant 2$. $\mathbb{F}_q$ 上秩为 $2i\,(0 \leqslant i \leqslant [\frac{n}{2}])$ 的 $n \times n$ 交错矩阵的个数为

$$K_i(n, q) = q^{i(i-1)} \frac{\prod\limits_{j=n-2i+1}^{n} (q^j - 1)}{\prod\limits_{j=1}^{i} (q^{2j} - 1)}. \tag{3.13}$$

证明 由前一节知, 在 $GL_n(\mathbb{F}_q)$ 的作用 (3.1) 之下, C_i 为一个 $GL_n(\mathbb{F}_q)$ 轨道. 取定 C_i 的一个元素

$$A = [K_i, 0^{(n-2i)}],\ K_i = \begin{pmatrix} 0 & I^{(i)} \\ -I^{(i)} & 0 \end{pmatrix}. \tag{3.14}$$

A 在 $GL_n(\mathbb{F}_q)$ 中的稳定子 G_A 由满足条件 $TA\,{}^tT = A$ 的矩阵 T 组成. 将 T 对应于 A 的形状分块

$$T = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{matrix} 2i \\ n-2i \end{matrix}, \quad (\text{列: } 2i,\ n-2i)$$

于是有下面的等式

$$AK_i\,{}^tA = K_i,\ CK_i\,{}^tA = 0.$$

由此可知 $A \in Sp_{2i}(K_i, \mathbb{F}_q)$; 特别地, A 是可逆的, 因而有 $C = 0$, $D \in GL_{n-2i}(\mathbb{F}_q)$. 这样, 我们有

$$|C_i| = \frac{|GL_n(\mathbb{F}_q)|}{|G_A|} = \frac{|GL_n(\mathbb{F}_q)|}{|Sp_{2i}(K_i, \mathbb{F}_q)||GL_{n-2i}(\mathbb{F}_q)|q^{2i(n-2i)}}.$$

进一步利用第 2 章中公式 (2.1) 及本节中的公式 (3.8) 即可得 (3.13). □

下面我们计算关系图 $\Gamma^{(1)}$ 的参数. 由定理 3.8 知 $\Gamma^{(1)}$ 的价

$$k_1 = K_1(n, q) = \frac{(q^n - 1)(q^{n-1} - 1)}{q^2 - 1}. \tag{3.15}$$

由定理 3.5 知, $\Gamma^{(1)}$ 是距离正则的, 所以只需计算参数 $c_i = p^i_{1\,i-1}$, $a_i = p^i_{1\,i}$ 和 $b_i = p^i_{1\,i+1}$. 又因为 $a_i + b_i + c_i = k_1$, 所以只要计算 c_i 和 b_i 就行了. 取定 $\Gamma^{(1)}$ 的两个顶点 B 和 A 使得 $\partial(B, A) = i$. 那么

$$c_i = |\Gamma^{(1)}_{i-1}(A) \cap \Gamma^{(1)}(B)|,$$
$$b_i = |\Gamma^{(1)}_{i+1}(A) \cap \Gamma^{(1)}(B)|.$$

不失一般性, 我们取 $B=0$ 及

$$A=\left[K_i,\, 0^{(m-2i)}\right],\quad K_i=\begin{pmatrix} 0 & I^{(i)} \\ -I^{(i)} & 0 \end{pmatrix}.$$

我们先计算 b_i. 令

$$\mathcal{M}=\{X\in C_1|\mathrm{rank}\,(X-A)=2i+2\}.$$

那么 $b_i=|\mathcal{M}|$. 设 $X\in\mathcal{M}$, 对应于 A 的形状做如下分块

$$X=\begin{pmatrix} U & V \\ -{}^tV & W \end{pmatrix}\begin{matrix} 2i \\ n-2i \end{matrix} \tag{3.16}$$
$$\qquad\begin{matrix} 2i & \quad n-2i \end{matrix}$$

我们断言: $\mathrm{rank}\,W=2$. 否则, 由于 $\mathrm{rank}\,X=2$ 就有 $W=0$ 并且 $\mathrm{rank}\,V\leqslant 1$. 这时存在 $T\in G_A$ 使得

$$TX\,{}^tT=\left(\begin{array}{c|c|c} U^* & {}^tv & 0 \\ \hline -v & 0 & \\ 0 & & 0 \end{array}\right).$$

这样就有 $\mathrm{rank}\,(X-A)=\mathrm{rank}\,(TX\,{}^tT-A)=2i$, 导致矛盾.

现在 $\mathrm{rank}\,W=2$. 存在 $T_1\in GL_{n-2}(\mathbb{F}_q)$ 使得

$$T_1W\,{}^tT_1=\left(\begin{array}{cc|c} 0 & 1 & \\ -1 & 0 & \\ \hline & & 0 \end{array}\right)\begin{matrix} 1 \\ 1 \\ n-2i-2 \end{matrix}\quad. \tag{3.17}$$

令 $T=[I^{(2i)},\,T_1]$, 那么 $TA\,{}^tT=A$, 而

$$TX\,{}^tT=\left(\begin{array}{c|cc|c} U & {}^tv_1 & {}^tv_2 & V_1 \\ \hline -v_1 & 0 & 1 & \\ -v_2 & -1 & 0 & \\ \hline -{}^tV_1 & & & 0 \end{array}\right)\begin{matrix} 2i \\ 1 \\ 1 \\ n-2i-2 \end{matrix}\quad.$$
$$\begin{matrix} 2i & 1 & 1 & n-2i-2 \end{matrix}$$

进一步由 $\mathrm{rank}\,X=2$ 可知 $V_1=0$, 并且 $U={}^tv_1v_2-{}^tv_2v_1$. U 由 v_1,v_2 所决定, 而 v_1,v_2 对于 X 的秩没有影响. 这就是说, 当 (3.16) 中的 W 取定为 (3.17) 之后, v_1,v_2 有 q^{4i} 个选取. 这样的 $X\in C_1$ 满足 $\mathrm{rank}\,(X-A)=2i+2$.

由于 W 的选取有 $K_1(n-2i,q)$ 个, 于是 $|\mathcal{M}|=q^{4i}K_1(n-2i,q)$. 利用公式 (3.13) 立得

$$b_i=q^{4i}\frac{(q^{n-2i}-1)(q^{n-2i-1}-1)}{q^2-1}.$$

我们有

定理 3.9　设 $n \geqslant 2$. $\mathbb{F}_q$ 上交错矩阵的距离正则图 $\Gamma^{(1)}$ 的参数为

$$b_i = \frac{q^{4i}(q^{n-2i}-1)(q^{n-2i-1}-1)}{q^2-1},\ 0 \leqslant i < \left[\frac{n}{2}\right], \tag{3.18}$$

$$c_i = \frac{q^{2(i-1)}(q^{2i}-1)}{q^2-1},\ 1 \leqslant i \leqslant \left[\frac{n}{2}\right]. \tag{3.19}$$

证明　b_i 的值上面已经算出. 至于 c_i, 直接计算比较复杂, 我们利用结合方案 $\mathrm{Alt}(n, q)$ 的参数关系和 b_i 的公式来导出. 由于

$$c_i = p^i_{1\,i-1} = k_{i-1}p^{i-1}_{1\,i}/k_i = k_{i-1}b_{i-1}/k_i,$$

利用 (3.13) 和 (3.18) 即可得 (3.19).　□

§3.3　p^k_{ij} 的递推计算

对于结合方案 $\mathrm{Alt}(n, q)$ 的交叉数 p^k_{ij}, 我们将给出它们的递推计算公式. 这些公式是逐步降阶的, 所以我们把 n 阶交错矩阵结合方案的交叉数记作 $p^k_{ij}(n)$. 相应地把 R_i 的价 k_i 记为 $k_i(n)$, 即 $k_i(n) = K_i(n, q)$.

定理 3.10　设 $0 < k < [\frac{n}{2}]$, $0 \leqslant i, j \leqslant [\frac{n}{2}]$. 我们有

$$\begin{aligned} p^k_{ij}(n) = & \sum_{\substack{0\leqslant 2\alpha\leqslant n-2k \\ 0\leqslant\beta\leqslant\min\{n-2k-2\alpha,2k\} \\ 0\leqslant 2s\leqslant\beta\leqslant k+s \\ 0\leqslant\alpha+\beta\leqslant\min\{i,j\}}} K_\alpha(n-2k, q)q^{2k(2\alpha+\beta)-\frac{1}{2}\beta(\beta+1)} \\ & \cdot n((n-2k-2\alpha)\times 2k;\ \beta, s)p^{k+s-\beta}_{i-\alpha-\beta\ j-\alpha-\beta}(2k-\beta). \end{aligned} \tag{3.20}$$

证明　取

$$B = 0,\ A = \left[\begin{pmatrix} 0 & I^{(k)} \\ -I^{(k)} & 0 \end{pmatrix}, 0^{(n-2k)}\right].$$

令

$$\mathcal{M}^k_{ij} = \{X \in \mathcal{K}(n, q) | \mathrm{rank}\, X = 2i,\ \mathrm{rank}\,(X-A) = 2j\},$$

那么 $p^k_{ij}(n) = |\mathcal{M}^k_{ij}|$. 对于任一 $X \in \mathcal{M}^k_{ij}$, 做相应于 A 的分块

$$X = \begin{pmatrix} U & V \\ -{}^tV & W \end{pmatrix} \begin{matrix} {\scriptstyle 2k} \\ {\scriptstyle n-2k} \end{matrix} . \tag{3.21}$$
$$\qquad\qquad {\scriptstyle 2k} \qquad {\scriptstyle n-2k}$$

我们按 X 的右下角块的秩将 $\mathcal{M}_{ij}^k$ 的元素分组. 对于 $0 \leqslant 2\alpha \leqslant n-2k$, 令

$$\mathcal{M}(\alpha) = \{X \in \mathcal{M}_{ij}^k | \operatorname{rank} W = 2\alpha\}.$$

那么有

$$|\mathcal{M}_{ij}^k| = \sum_{0 \leqslant 2\alpha \leqslant n-2k} |\mathcal{M}(\alpha)|. \tag{3.22}$$

设 $\mathcal{M}(\alpha) \neq \varnothing$. 任取其中一个元素 X, 设其有形状 (3.21). 由于 $\operatorname{rank} W = 2\alpha$, 所以存在 $P \in GL_{n-2k}(\mathbb{F}_q)$ 使得

$$PW\,{}^tP = \left[\begin{pmatrix} 0 & I^{(\alpha)} \\ -I^{(\alpha)} & 0 \end{pmatrix}, 0^{(n-2k-2\alpha)}\right].$$

令 $T = [I^{(2k)}, P]$, 那么 T 导出的变换使 A 不动, 而将 X 变成

$$TX\,{}^tT = \begin{pmatrix} U & V\,{}^tP \\ -P\,{}^tV & PW\,{}^tP \end{pmatrix}.$$

并把 $\mathcal{M}(\alpha)$ 映到自身. 令 $\mathcal{M}_1$ 为 $\mathcal{M}(\alpha)$ 中全体形如

$$\begin{pmatrix} U & V_1 & V_2 & V_3 \\ -{}^tV_1 & 0 & I^{(\alpha)} & 0 \\ -{}^tV_2 & -I^{(\alpha)} & 0 & 0 \\ -{}^tV_3 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} 2k \\ \alpha \\ \alpha \\ n-2k-2\alpha \end{matrix} \tag{3.23}$$
$$\begin{matrix} 2k & \alpha & \alpha & n-2k-2\alpha \end{matrix}$$

的元素做成的集合. 于是我们有

$$|\mathcal{M}(\alpha)| = K_\alpha(n-2k, q)|\mathcal{M}_1|. \tag{3.24}$$

现在, 施行由矩阵

$$\left[\begin{pmatrix} I^{(2k)} & -V_2 & V_1 \\ & I^{(\alpha)} & 0 \\ & & I^{(\alpha)} \end{pmatrix}, I^{(n-2k-2\alpha)}\right]$$

导出的变换, 它将矩阵 (3.23) 变成

$$\begin{pmatrix} U^* & 0 & 0 & V_3 \\ 0 & 0 & I^{(\alpha)} & 0 \\ 0 & -I^{(\alpha)} & 0 & 0 \\ -{}^tV_3 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} 2k \\ \alpha \\ \alpha \\ n-2k-2\alpha \end{matrix} \tag{3.25}$$

而使 A 不动, 同时使 $\mathcal{M}_1$ 不变. 我们令 $\mathcal{M}_2$ 表示 $\mathcal{M}_1$ 中全体形如 (3.25) 的矩阵做成的集合, 于是有

$$|\mathcal{M}_1| = q^{4k\alpha}|\mathcal{M}_2|. \tag{3.26}$$

进一步, 我们对 $\mathcal{M}_2$ 中的矩阵按其左下块 ${}^tV_3$ 关于 K_k 的类型来分组. 令 $\mathcal{M}(\beta,\, s)$ 表示 $\mathcal{M}_2$ 中左下角块 ${}^tV_3$ 关于 K_k 的类型为 $(\beta,\, s)$ 的那些矩阵的集合, 于是有

$$|\mathcal{M}_2| = \sum_{\substack{0\leqslant\beta\leqslant\min\{n-2k-2\alpha,2k\}\\ 0\leqslant 2s\leqslant\beta\leqslant k+s}} |\mathcal{M}(\beta,\, s)|. \tag{3.27}$$

设 $\mathcal{M}(\beta,\, s)\neq\varnothing$, 任取其中一个元素 X, 它有形状 (3.25). 由于 ${}^tV_3$ 关于 K_k 为 $(\beta,\, s)$ 型的, 所以存在 $P\in Sp_{2k}(K_k,\, \mathbb{F}_q)$ 及 $Q\in GL_{n-2k-2\alpha}(\mathbb{F}_q)$ 使得

$${}^tV\,{}^tP = Q\begin{pmatrix} I^{(s)} & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & I^{(s)} & 0 & 0\\ 0 & I^{(\beta-2s)} & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}\begin{matrix} s\\ s\\ \beta-2s\\ n-2k-2\alpha-\beta \end{matrix}$$
$$\qquad\qquad\qquad\quad s \qquad \beta-2s \qquad k+s-\beta \qquad s \qquad \beta-2s \qquad k+\beta-s$$

注意到 $P\in Sp_{2k}(K_k,\, \mathbb{F}_q)$ 当且仅当 ${}^tP\in Sp_{2k}(K_k,\, \mathbb{F}_q)$. 令

$$T = [P,\, I^{(2\alpha)},\, Q^{-1}],$$

那么由 T 导出的变换使 A 不动, 而将 X 变到

$$\left(\begin{array}{ccc|ccc|cc|cccc}
U_{11} & U_{12} & U_{13} & U_{14} & U_{15} & U_{16} & & & I^{(s)} & 0 & 0 & 0\\
-{}^tU_{12} & U_{22} & U_{23} & U_{24} & U_{25} & U_{26} & & & 0 & 0 & I^{(\beta-2s)} & 0\\
-{}^tU_{13} & -{}^tU_{23} & U_{33} & U_{34} & U_{35} & U_{36} & \multicolumn{2}{c|}{0} & 0 & 0 & 0 & 0\\
\cline{1-6}
-{}^tU_{14} & -{}^tU_{24} & -{}^tU_{34} & U_{44} & U_{45} & U_{46} & & & 0 & I^{(s)} & 0 & 0\\
-{}^tU_{15} & -{}^tU_{25} & -{}^tU_{35} & -{}^tU_{45} & U_{55} & U_{56} & & & 0 & 0 & 0 & 0\\
-{}^tU_{16} & -{}^tU_{26} & -{}^tU_{36} & -{}^tU_{46} & -{}^tU_{56} & U_{66} & & & 0 & 0 & 0 & 0\\
\hline
\multicolumn{6}{c|}{\multirow{2}{*}{0}} & 0 & I^{(\alpha)} & \multicolumn{4}{c}{\multirow{2}{*}{0}}\\
\multicolumn{6}{c|}{} & -I^{(\alpha)} & 0 & \multicolumn{4}{c}{}\\
\hline
-I^{(s)} & 0 & 0 & 0 & 0 & 0 & & & & & & \\
0 & 0 & 0 & -I^{(s)} & 0 & 0 & \multicolumn{2}{c|}{0} & \multicolumn{4}{c}{0}\\
0 & -I^{(\beta-2s)} & 0 & 0 & 0 & 0 & & & & & & \\
0 & 0 & 0 & 0 & 0 & 0 & & & & & &
\end{array}\right), \tag{3.28}$$

并且将 $\mathcal{M}(\beta, s)$ 变到自身. 令 $\mathcal{M}_3$ 表示 $\mathcal{M}(\beta, s)$ 中全体形如 (3.28) 的矩阵作成的集合. 于是我们有

$$|\mathcal{M}(\beta, s)| = n((n-2k-2\alpha)\times 2k;\ \beta, s)|\mathcal{M}_3|. \tag{3.29}$$

设 $X \in \mathcal{M}_3$, 那么对 X 施行适当的合同变换可将第 1, 2, 4 行和相应列上的子块 U_{ij} 化为 0, 即将 X 变到

$$\left(\begin{array}{ccc|ccc|cc|cccc}
0 & 0 & 0, & 0 & 0 & 0 & & & I^{(s)} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & & & 0 & 0 & I^{(\beta-2s)} & 0 \\
0 & 0 & U_{33} & 0 & U_{35} & U_{36} & \multicolumn{2}{c|}{0} & 0 & 0 & 0 & 0 \\
\cline{1-6}
0 & 0 & 0 & 0 & 0 & 0 & & & 0 & I^{(s)} & 0 & 0 \\
0 & 0 & -{}^tU_{35} & 0 & U_{55} & U_{56} & & & 0 & 0 & 0 & 0 \\
0 & 0 & -{}^tU_{36} & 0 & -{}^tU_{56} & U_{66} & & & 0 & 0 & 0 & 0 \\
\hline
\multicolumn{6}{c|}{\multirow{2}{*}{0}} & 0 & I^{(\alpha)} & \multicolumn{4}{c}{\multirow{2}{*}{0}} \\
\multicolumn{6}{c|}{} & -I^{(\alpha)} & 0 & \multicolumn{4}{c}{} \\
\hline
-I^{(s)} & 0 & 0 & 0 & 0 & 0 & & & & & & \\
0 & 0 & 0 & -I^{(s)} & 0 & 0 & \multicolumn{2}{c|}{0} & \multicolumn{4}{c}{0} \\
0 & -I^{(\beta-2s)} & 0 & 0 & 0 & 0 & & & & & & \\
0 & 0 & 0 & 0 & 0 & 0 & & & & & &
\end{array}\right) \tag{3.30}$$

这个变换也使 A 不动, 并且把 $\mathcal{M}_3$ 映到自身. 令 $\mathcal{M}_4$ 表示 $\mathcal{M}_3$ 中全体形如 (3.30) 的矩阵作成的集合, 于是有

$$|\mathcal{M}_3| = q^{2k\beta-\frac{1}{2}\beta(\beta+1)}|\mathcal{M}_4|. \tag{3.31}$$

现在, 我们计算 $|\mathcal{M}_4|$. 对于 $\mathcal{M}_4$ 中每个矩阵 X, 它的形状如 (3.30), 令

$$U^* = \begin{pmatrix} U_{33} & U_{35} & U_{36} \\ -{}^tU_{35} & U_{55} & U_{56} \\ -{}^tU_{36} & -{}^tU_{56} & U_{66} \end{pmatrix} \begin{matrix} k+s-\beta \\ \beta-2s \\ k+s-\beta \end{matrix}.$$

再令

$$A^* = \begin{pmatrix} 0 & 0 & I^{(k+s-\beta)} \\ 0 & 0 & 0 \\ -I^{(k+s-\beta)} & 0 & 0 \end{pmatrix} \begin{matrix} k+s-\beta \\ \beta-2s \\ k+s-\beta \end{matrix}.$$

显然,$\operatorname{rank} A^* = 2(k+s-\beta)$. 由 $\operatorname{rank} X = 2i$ 和 $\operatorname{rank}(X-A) = 2j$ 可知

$$\operatorname{rank} U^* = 2(i-\alpha-\beta) \text{ 及 } \operatorname{rank}(U^*-A^*) = 2(j-\alpha-\beta). \tag{3.32}$$

每个满足条件 (3.32) 的交错矩阵 U^* 可以唯一地扩充成形如 (3.30) 的交错矩阵 X. 因此我们有

$$|\mathcal{M}_4| = p^{k+s-\beta}_{i-\alpha-\beta,j-\alpha-\beta}(2k-\beta). \tag{3.33}$$

这样, 由 (3.22), (3.24), (3.26), (3.27), (3.29), (3.31) 和 (3.33) 就得到 (3.20). 定理得证. □

如果 $k=[\frac{n}{2}]$ 而 i, j 中有小于 $[\frac{n}{2}]$ 的, 比方说 $i<[\frac{n}{2}]$. 这时我们可以利用等式 $p^k_{ij}=\frac{k_i}{k_k}p^i_{kj}$ 来计算. 当 $i=j=k=[\frac{n}{2}]$ 时, 可利用命题 1.1(v) 计算 $p^{[\frac{n}{2}]}_{[\frac{n}{2}][\frac{n}{2}]}(n)$.

下一节中我们将给出 $p^{[\frac{n}{2}]}_{[\frac{n}{2}][\frac{n}{2}]}(n)$ 的一个降阶递推算法.

§3.4　交叉数计算续

在这一节中, 我们给出计算 $p^m_{m\,m}(2m+1)$ 和 $p^m_{m\,m}(2m)$ 的降阶递推公式. 先看 n 为奇数的情形. 我们有

定理 3.11　设 $n=2m+1$. 于是 $[\frac{n}{2}]=m$. 那么

$$p^m_{m\,m}(2m+1) = p^m_{m\,m}(2m) + q^{2m-1}(q^{2m}-1)p^{m-1}_{m-1\,m-1}(2m-1). \tag{3.34}$$

证明　令

$$K=[K_m,\,0],\ K_m=\begin{pmatrix} 0 & I^{(m)} \\ -I^{(m)} & 0 \end{pmatrix}.$$

再令

$$\mathcal{M}=\{X\in\mathcal{K}(2m+1,\,q)|\text{rank}X=\text{rank}\,(X-K)=2m\}.$$

于是 $p^m_{m\,m}(2m+1)=|\mathcal{M}|$.

现在, 对于每个 $X\in\mathcal{M}$, 相应于 K 的形状分块

$$X=\left(\begin{array}{cc|c} X_{11} & X_{12} & u_1 \\ -{}^tX_{12} & X_{22} & u_2 \\ \hline -{}^tu_1 & -{}^tu_2 & 0 \end{array}\right)\begin{array}{l} m \\ m \\ 1 \end{array}. \tag{3.35}$$

令 $\mathcal{M}_0$ 为 $\mathcal{M}$ 中 $({}^tu_1,\,{}^tu_2)=0$ 的那些交错矩阵的集合. 记

$$Y=\begin{pmatrix} X_{11} & X_{12} \\ -{}^tX_{12} & X_{22} \end{pmatrix}.$$

由于 $\text{rank}\,X=2m$ 和 $\text{rank}\,(X-K)=2m$, 这时有 $\text{rank}\,Y=2m$ 和 $\text{rank}\,(Y-K_m)=2m$. 因而有

$$|\mathcal{M}_0| = p^m_{m\,m}(2m). \tag{3.36}$$

再令 $\mathcal{M}_1=\mathcal{M}\backslash\mathcal{M}_0$. 任取一个 $X\in\mathcal{M}_1$, 其形状如 (3.35), 由于 $({}^tu_1, {}^tu_2)\neq 0$, 存在 $P\in Sp_{2m}(K_m, \mathbb{F}_q)$ 使得

$$({}^tu_1, {}^tu_2){}^tP=(1, 0, \cdots, 0).$$

令 $T=[P, 1]$. 那么由 T 导出的变换使 K 不动, 而将 X 映到矩阵

$$\left(\begin{array}{ccc|c} 0 & y_{12} & y_{13} & 1 \\ -{}^ty_{12} & Y_{22} & Y_{23} & 0 \\ -{}^ty_{13} & -{}^tY_{23} & Y_{33} & 0 \\ \hline -1 & 0 & 0 & 0 \end{array}\right)\begin{array}{l} 1 \\ m-1 \\ m \\ 1 \end{array}, \tag{3.37}$$

并且将 $\mathcal{M}_1$ 映到自身. 令 $\mathcal{M}_2$ 为 $\mathcal{M}_1$ 中全体形如 (3.37) 的矩阵所成的集合, 于是有

$$|\mathcal{M}_1|=(q^{2m}-1)|\mathcal{M}_2|. \tag{3.38}$$

设 $X\in\mathcal{M}_2$, 它有形状 (3.37). 那么有合同变换将 X 变到

$$\left(\begin{array}{ccc|c} 0 & 0 & 0 & 1 \\ 0 & Y_{22} & Y_{23} & 0 \\ 0 & -{}^tY_{23} & Y_{33} & 0 \\ \hline -1 & 0 & 0 & 0 \end{array}\right) \tag{3.39}$$

而使 K 不动, 并且将 $\mathcal{M}_2$ 映到自身. 令 $\mathcal{M}_3$ 为 $\mathcal{M}_2$ 中全体形如 (3.39) 的矩阵所成的集合, 那么有

$$|\mathcal{M}_2|=q^{2m-1}|\mathcal{M}_3|. \tag{3.40}$$

现在, 对于 $X\in\mathcal{M}_3$, 它有形状 (3.39), 令

$$Y^*=\left(\begin{array}{c|c} Y_{22} & Y_{23} \\ \hline -{}^tY_{23} & Y_{33} \end{array}\right)\begin{array}{l} m-1 \\ m \end{array},$$

再令

$$K^*=\left(\begin{array}{c|cc} 0 & 0 & I^{(m-1)} \\ \hline 0 & & \\ -I^{(m-1)} & & 0 \end{array}\right)\begin{array}{l} m-1 \\ \\ m \end{array},$$

那么 $\operatorname{rank} K^*=2(m-1)$. 由 $\operatorname{rank} X=2m$ 及 $\operatorname{rank}(X-K)=2m$ 可知

$$\operatorname{rank} Y^*=2(m-1) \text{ 及 } \operatorname{rank}(Y^*-K^*)=2(m-1).$$

于是有

$$|\mathcal{M}_3| = p^{m-1}_{m-1\,m-1}(2m-1). \tag{3.41}$$

这样, 由 (3.36), (3.38), (3.40) 和 (3.41) 立得 (3.34). □

现在讨论 n 为偶数的情形. 为了书写简单, 我们设 $n = 2m+2$, $m \geqslant 1$. 我们有

定理 3.12 设 $n = 2m+2$, $m \geqslant 1$. 于是 $[\frac{n}{2}] = m+1$. 那么

$$p^{m+1}_{m+1\,m+1}(2m+2) = q^{2m}(q^{2m+1} - q^{2m} - 1)p^{m}_{m\,m}(2m)$$
$$+q^{2m}(q^{2m}-1)p^{m-1}_{m\,m}(2m). \tag{3.42}$$

证明 令

$$K = \left[K_m, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right], \; K_m = \begin{pmatrix} 0 & I^{(m)} \\ -I^{(m)} & 0 \end{pmatrix}.$$

再令

$$\mathcal{M} = \{X \in \mathcal{K}(2m+2, q) | \text{rank}\, X = \text{rank}\,(X-K) = 2m+2\}.$$

于是 $p^{m+1}_{m+1\,m+1}(2m+2) = |\mathcal{M}|$.

现在, 对于每个 $X \in \mathcal{M}$, 相应于 K 的形状作如下分块

$$X = \left(\begin{array}{cc|cc} X_{11} & X_{12} & v_1 & u_1 \\ -{}^tX_{12} & X_{22} & v_2 & u_2 \\ \hline -{}^tv_1 & -{}^tv_2 & 0 & w \\ -{}^tu_1 & -{}^tu_2 & -w & 0 \end{array}\right) \begin{array}{l} m \\ m \\ 1 \\ 1 \end{array}.$$

区分 $({}^tu_1, {}^tu_2) = 0$ 和 $({}^tu_1, {}^tu_2) \neq 0$ 的两种情形并讨论之. 令 $\mathcal{M}_0$ 为 $\mathcal{M}$ 中 $({}^tu_1, {}^tu_2) = 0$ 的那些矩阵所成的集合. 每个 $X \in \mathcal{M}_0$ 有形状

$$X = \left(\begin{array}{cc|cc} X_{11} & X_{12} & v_1 & 0 \\ -{}^tX_{12} & X_{22} & v_2 & 0 \\ \hline -{}^tv_1 & -{}^tv_2 & 0 & w \\ 0 & 0 & -w & 0 \end{array}\right). \tag{3.43}$$

由于 rank $X = 2m+2$, 所以 $w \neq 0$. 又因为 $\text{rank}\,(X-K) = 2m+2$, 所以 $w \neq 1$. 显然, v_1, v_2 对于矩阵 (3.43) 的秩没有影响. 记

$$Y = \begin{pmatrix} X_{11} & X_{12} \\ -{}^tX_{12} & X_{22} \end{pmatrix},$$

那么 $\text{rank}\, Y = 2m$, 并且 $\text{rank}\,(Y - K_m) = 2m$. 于是我们有

$$|\mathcal{M}_0| = q^{2m}(q-2)p^{m}_{m\,m}(2m). \tag{3.44}$$

令 $\mathcal{M}_1 = \mathcal{M}\backslash\mathcal{M}_0$. 任取一个 $X \in \mathcal{M}_1$, 它的分块中 $({}^tu_1, {}^tu_2) \neq 0$, 那么存在 $P \in Sp_{2m}(K_m, \mathbb{F}_q)$ 使得 $({}^tu_1, {}^tu_2){}^tP = (1, 0, \cdots, 0)$. 令 $T = [P, I^{(2)}]$, 那么由 T 给出的合同变换使 K 不动, 而将 X 变到

$$\left(\begin{array}{ccc|cc} 0 & y_{11} & y_{12} & v & 1 \\ -{}^ty_{11} & Y_{11} & Y_{12} & \overline{v}_1 & 0 \\ -{}^ty_{12} & -{}^tY_{12} & Y_{22} & \overline{v}_2 & 0 \\ \hline -v & -{}^t\overline{v}_1 & -{}^t\overline{v}_2 & 0 & w \\ -1 & 0 & 0 & -w & 0 \end{array}\right) \begin{array}{l} 1 \\ m-1 \\ m \\ 1 \\ 1 \end{array}, \tag{3.45}$$

这里 $v \in \mathbb{F}_q$, $y_{11} = (y_2, \cdots, y_m) \in \mathbb{F}_q^{(m-1)}$, $y_{12} = (y_{m+1}, \cdots, y_{2m}) \in \mathbb{F}_q^{(m)}$. 这个变换显然将 $\mathcal{M}_1$ 变到 $\mathcal{M}_1$. 令 $\mathcal{M}_2$ 为 $\mathcal{M}_1$ 中全体形如 (3.45) 的矩阵所成集合, 于是

$$|\mathcal{M}_1| = (q^{2m} - 1)|\mathcal{M}_2|. \tag{3.46}$$

现在, 取定 (3.45) 中的 y_{11}, y_{12}, v 和 w. 考虑 $\mathcal{M}_2$ 中相应那些矩阵 X, 对它们施行如下的合同变换: 将第 1 行乘以 $-w$ 后加到第 $2m+1$ 行, 将第 1 列乘以 $-w$ 后加到第 $2m+1$ 列, 那么 X 变到

$$\left(\begin{array}{ccc|cc} 0 & y_{11} & y_{12} & v & 1 \\ -{}^ty_{11} & Y_{11} & Y_{12} & \widetilde{v}_1 & 0 \\ -{}^ty_{12} & -{}^tY_{12} & Y_{22} & \widetilde{v}_2 & 0 \\ \hline -v & -{}^t\widetilde{v}_1 & -\widetilde{v}_2 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \end{array}\right),$$

这里 $\widetilde{v}_1 = \overline{v}_1 + w\,{}^ty_{11}$, $\widetilde{v}_2 = \overline{v}_2 + w\,{}^ty_{12}$. 令

$$Z = \begin{pmatrix} Y_{11} & Y_{12} & \widetilde{v}_1 \\ -{}^tY_{12} & Y_{22} & \widetilde{v}_2 \\ -{}^t\widetilde{v}_1 & -{}^t\widetilde{v}_2 & 0 \end{pmatrix} \begin{array}{l} m-1 \\ m \\ 1 \end{array}.$$

由于 $\operatorname{rank} X = 2m+2$ 知 $\operatorname{rank} Z = 2m$.

相应地考虑那些矩阵 X 与 K 的差, 它们有形状

$$X - K = \left(\begin{array}{ccc|cc} 0 & y_{11} & y_{12} - (1,0) & v & 1 \\ -{}^ty_{11} & Y_{11} & Y_{12} - (0, I^{(m-1)}) & \overline{v}_1 & 0 \\ -{}^ty_{12} + \begin{pmatrix} 1 \\ 0 \end{pmatrix} & -{}^tY_{12} + \begin{pmatrix} 0 \\ I^{(m-1)} \end{pmatrix} & Y_{22} & \overline{v}_2 & 0 \\ \hline -v & -{}^t\overline{v}_1 & -{}^t\overline{v}_2 & 0 & w-1 \\ -1 & 0 & 0 & -w+1 & 0 \end{array}\right).$$

现在, 将它的第 1 行和第 1 列分别乘以 $1-w$ 后加到第 $2m+1$ 行和第 $2m+1$ 列上得到矩阵

$$\left(\begin{array}{ccc|cc} 0 & y_{11} & y_{12}-(1,0) & v & 1 \\ -{}^ty_{11} & Y_{11} & Y_{12}-(0,I^{(m-1)}) & \widehat{v}_1 & 0 \\ -{}^ty_{12}+\begin{pmatrix}1\\0\end{pmatrix} & -{}^tY_{12}+\begin{pmatrix}0\\I^{(m-1)}\end{pmatrix} & Y_{22} & \widehat{v}_2 & 0 \\ \hline -v & -{}^t\widehat{v}_1 & -{}^t\widehat{v}_2 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \end{array}\right),$$

这里

$$\widehat{v}_1=\overline{v}_1+(w-1)\,{}^ty_{11}=\widetilde{v}_1-{}^ty_{11},$$
$$\widehat{v}_2=\overline{v}_2+(w-1)\,{}^ty_{12}=\widetilde{v}_2-{}^ty_{12}+(w-1)\begin{pmatrix}1\\0\end{pmatrix}.$$

令

$$\widetilde{Z}=\begin{pmatrix} Y_{11} & Y_{12}-(0\,I^{(m-1)}) & \widehat{v}_1 \\ -{}^tY_{12}+\begin{pmatrix}0\\I^{(m-1)}\end{pmatrix} & Y_{22} & \widehat{v}_2 \\ -{}^t\widehat{v}_1 & -{}^t\widehat{v}_2 & 0 \end{pmatrix}.$$

由于 $\operatorname{rank}(X-K)=2m+2$ 有 $\operatorname{rank}\widetilde{Z}=2m$. 令

$$\widetilde{K}=\left(\begin{array}{cccc|cccc|c} & & & & 0 & 1 & & & y_2 \\ & & & & 0 & & 1 & & y_3 \\ & & & & \vdots & & & \ddots & \vdots \\ & & & & 0 & & & 1 & y_m \\ \hline 0 & 0 & \cdots & 0 & & & & & y^* \\ -1 & & & & & & & & y_{m+2} \\ & -1 & & & & & & & \vdots \\ & & \ddots & & & & & & \\ & & & -1 & & & & & y_{2m} \\ \hline -y_2 & -y_3 & \cdots & y_m & -y^* & -y_{m+2} & \cdots & -y_{2m} & 0 \end{array}\right),$$

这里 $y^*=y_{m+1}-w+1$. 那么

$$\operatorname{rank}\widetilde{K}=\begin{cases} 2m, & \text{如果 } w\neq y_{m+1}+1, \\ 2m-2, & \text{如果 } w=y_{m+1}+1. \end{cases}$$

进一步, 由 $\widetilde{Z}=Z-\widetilde{K}$ 可知, 当 $w\neq y_{m+1}+1$ 时, Z 的个数为 $p_{m\,m}^{m}(2m)$; 而当 $w=y_{m+1}+1$ 时, Z 的个数为 $p_{m\,m}^{m-1}(2m)$. 对于这样得到的每个 Z, 我们可以相应得

到 $\mathcal{M}_2$ 中的一个矩阵 X. 于是有

$$|\mathcal{M}_2| = q^{2m}(q-1)p_{m\,m}^{m}(2m) + q^{2m}p_{m\,m}^{m-1}(2m). \tag{3.47}$$

于是由 (3.44), (3.46) 和 (3.47) 立得 (3.42). □

§3.5 交错矩阵结合方案的自对偶性

在这一节中, 我们证明结合方案 Alt(n, q) 是自对偶的.

设 $n \geqslant 2$, 结合方案 Alt(n, q) 的类数为 $[\frac{n}{2}]$, 结合关系

$$R_i = \{(X, Y)|Y - X \in C_i\}, \quad i = 0, 1, \cdots, \left[\frac{n}{2}\right],$$

这里 C_i 为 $\mathbb{F}_q$ 上全体秩为 $2i$ 的 $n \times n$ 交错矩阵所成集合. $\mathbb{F}_q$ 上全体 $n \times n$ 交错矩阵对于矩阵加法作成一个交换群, 我们记作 $\mathcal{K}(n, q)$. 它的特征标群记作 $\mathcal{K}(n, q)^*$.

现在, 任意取定基域的加法群 $(\mathbb{F}_q, +)$ 在复数域 $\mathbb{C}$ 上的一个非平凡不可约特征标 χ. 对于每个交错阵 $A = (a_{ij}) \in \mathcal{K}(n, q)$, 我们定义映射

$$\begin{aligned} \phi_A : \mathcal{K}(n, q) &\longrightarrow \mathbb{C} \\ X = (x_{ij}) &\longmapsto \chi(\textstyle\sum_{i<j} a_{ij}x_{ij}). \end{aligned} \tag{4.48}$$

那么 ϕ_A 是 $\mathcal{K}(n, q)$ 的一个特征标, 并且有

$$\phi_{A+B} = \phi_A\phi_B.$$

命题 3.13 设 $A, B \in \mathcal{K}(n, q)$, 那么 $\phi_A = \phi_B$ 当且仅当 $A = B$. 于是映射 $A \mapsto \phi_A$ 是 $\mathcal{K}(n, q)$ 到 $\mathcal{K}(n, q)^*$ 的一个同构.

证明 与命题 2.12 的证明类似, 故从略. □

命题 3.14 对于 $A, X \in \mathcal{K}(n, q)$, $P \in GL_n(\mathbb{F}_q)$, 恒有

$$\phi_A(PX\,{}^tP) = \phi_{{}^tPAP}(X). \tag{3.49}$$

证明 设 $A = (a_{ij})$, $X = (x_{ij})$, 再设 $P = (p_{ij})$, $PX\,{}^tP = (x^*_{ij})$, ${}^tPAP = (a^*_{ij})$. 那么 $x^*_{ij} = \sum_{k=1}^{n}\sum_{l=1}^{n} p_{ik}x_{kl}p_{jl}$, $a^*_{ij} = \sum_{k=1}^{n}\sum_{l=1}^{n} p_{ki}a_{kl}p_{lj}$. 注意到 A, X, (x^*_{ij}) 和 (a^*_{ij}) 均为交错矩阵, 易见

$$\sum_{i<j} a_{ij}x^*_{ij} = \sum_{i<j} a^*_{ij}x_{ij}.$$

于是立得 (3.49). □

令 $\mathbb{C}_i$ 表示等价类 C_i 在 $\mathcal{K}(n,q)$ 的群代数 $\mathbb{C}\mathcal{K}(n,q)$ 中的形式和, $\mathfrak{S}$ 是由 $\mathbb{C}_0$, $\mathbb{C}_1, \cdots, \mathbb{C}_{[\frac{n}{2}]}$ 生成的 S 环, 由 $\mathfrak{S}$ 确定的结合方案 $\mathfrak{X}(\mathfrak{S})$ 就是 $\mathrm{Alt}(n,q)$. 令

$$\phi_A(\mathbb{C}_i) = \sum_{X\in C_i} \phi_A(X),\ i = 0, 1, \cdots, \left[\frac{n}{2}\right]. \tag{3.50}$$

由定理 1.16 知, $\phi_A(\mathbb{C}_i)$ 是 $\mathrm{Alt}(n,q)$ 的邻接矩阵 A_i 的特征值, 属于特征向量 ϕ_A. 由命题 3.14 知, 对于 $A, B \in \mathcal{K}(n,q)$, 如果

$$\phi_A(\mathbb{C}_i) = \phi_B(\mathbb{C}_i), \qquad i = 0, 1, \cdots, \left[\frac{n}{2}\right],$$

那么 A 和 B 在同一个等价类中. 于是定理 1.16 中在 $\mathcal{K}(n,q)^*$ 上确定的等价类 Y_j 恰为

$$Y_j = \{\phi_A | A \in C_j\},\ j = 0, 1, \cdots, \left[\frac{n}{2}\right].$$

相应地得到 $\mathcal{K}(n,q)^*$ 上的一个 S 环 $\mathfrak{S}^*$. 由 $\mathfrak{S}^*$ 确定的结合方案 $\mathfrak{X}(\mathfrak{S}^*)$ 和 $\mathrm{Alt}(n,q)$ 是形式对偶的.

现在, 映射 $A \mapsto \phi_A$ 是 $\mathcal{K}(n,q)$ 到 $\mathcal{K}(n,q)^*$ 的一个同构对应, 它诱导出结合方案 $\mathrm{Alt}(n,q)$ 和 $\mathfrak{X}(\mathfrak{S}^*)$ 的一个同构. 因此, 我们得到

定理 3.15　交错矩阵结合方案 $\mathrm{Alt}(n,q)$ 是自对偶的.

实际上, 由 (3.49) 和 (3.50) 及定理 1.16 可知, 结合方案 $\mathrm{Alt}(n,q)$ 的第一特征值矩阵 $P = (p_i(j))$ 的 (j,i) 位置元素为

$$p_i(j) = \phi_A(\mathbb{C}_i) = \sum_{X\in C_i} \phi_A(X),\ A \in C_j.$$

由定义 (3.48) 可知, $\phi_A(X) = \phi_X(A)$. 通过计算 $\sum_{A\in C_j}\sum_{X\in C_i}\phi_A(X)$ 可得

$$k_j p_i(j) = k_i p_j(i).$$

由此即可导出

$$P^2 = |K(n,q)|I.$$

由定理 3.6 和定理 3.15 可得

定理 3.16　交错矩阵结合方案 $\mathrm{Alt}(n,q)$ 是 P 和 Q 多项式的.

§3.6　交错矩阵结合方案的自同构

关于交错矩阵结合方案的自同构, 我们有下面的

定理 3.17 设 $n \geqslant 4$. $\mathbb{F}_q$ 上 n 阶交错矩阵结合方案 Alt(n, q) 的自同构具有如下的形状:

$$X \mapsto \xi P X^{\sigma}\,{}^{t}P + A_0,\ \forall X \in \mathcal{K}(n,q), \tag{3.51}$$

这里当 q 为偶数时, $\xi = 1$; 当 q 为奇数时, $\xi = 1$ 或 z(z 为 $\mathbb{F}_q$ 中取定的一个非平方元), $P \in GL_n(\mathbb{F}_q)$, σ 是 $\mathbb{F}_q$ 的一个自同构, $A_0 \in \mathcal{K}(n,q)$; 当 $n = 4$ 时, 除了上述形状的自同构以外, 还有如下形状的自同构

$$X \mapsto \xi P\,(X^{*})^{\sigma}\,{}^{t}P + A_0, \tag{3.52}$$

这里 ξ, P, σ, A_0 如上所述, X^* 如下定义

$$\begin{pmatrix} 0 & x_{12} & x_{13} & x_{14} \\ -x_{12} & 0 & x_{23} & x_{24} \\ -x_{13} & -x_{23} & 0 & x_{34} \\ -x_{14} & -x_{24} & -x_{34} & 0 \end{pmatrix}^{*} = \begin{pmatrix} 0 & x_{12} & x_{13} & x_{23} \\ -x_{12} & 0 & x_{14} & x_{24} \\ -x_{13} & -x_{14} & 0 & x_{34} \\ -x_{23} & -x_{24} & -x_{34} & 0 \end{pmatrix}.$$

证明 设 $q = p^t$, 这里 p 为一素数. 由定理 3.8, 结合方案 Alt(n, q) 的价 $k_i = K_i(n, q)$ 所含素数 p 的幂为 $p^{ti(i-1)}$, $i = 1, \cdots, [\frac{n}{2}]$, 它们皆不同, 所以 $k_1, \cdots, k_{[\frac{n}{2}]}$ 两两不等. 于是由推论 1.28(i), Alt(n, q) 的每个自同构都是内自同构, 即是说,Alt(n, q) 的自同构都是每个关系图的自同构.

再由定理 3.5 知,Alt(n, q) 的关系图 $\Gamma^{(1)}$ 是距离正则的, 因而 $\Gamma^{(1)}$ 的自同构也是每个关系图 $\Gamma^{(i)}$ ($i \neq 0$) 的自同构. 于是有 Aut(Alt(n, q)) =Aut $\Gamma^{(1)}$.

最后, 由交错矩阵仿射几何基本定理 [16] 知, 图 $\Gamma^{(1)}$ 的自同构必为形状 (3.51) 或者 (3.52) (当 $n = 4$ 时). 于是定理得证. □

注意, 结合方案 Alt(2, q) 和 Alt(3, q) 都是平凡的.

第四章　Hermite 矩阵的结合方案

§4.1　Hermite 矩阵结合方案及其本原性和 P 多项式性质

令 $\mathbb{F}_{q^2}$ 为 q^2 个元素的有限域, 这里 q 是一个素数的幂. $\mathbb{F}_{q^2}$ 有一个对合自同构, 即阶为 2 的自同构:

$$a \longmapsto \overline{a} = a^q, \ \forall a \in \mathbb{F}_{q^2},$$

这个自同构的固定子域就是 $\mathbb{F}_q$. 考虑从 $\mathbb{F}_{q^2}$ 的加法群到 $\mathbb{F}_q$ 的加法群的如下映射:

$$\begin{aligned} \phi : (\mathbb{F}_{q^2}, +) &\longrightarrow (\mathbb{F}_q, +) \\ x &\longmapsto x + \overline{x}, \end{aligned}$$

这是一个群同态, 它的核 $\operatorname{Ker}\phi$ 由满足条件 $x + \overline{x} = x + x^q = 0$ 的元素组成, 于是有 $|\operatorname{Ker}\phi| \leqslant q$. 另一方面, $|\operatorname{Im}\phi| \leqslant |\mathbb{F}_q| = q$. 于是由 $|\mathbb{F}_{q^2}| = |\operatorname{Ker}\phi||\operatorname{Im}\phi|$ 及 $|\mathbb{F}_{q^2}| = q^2$ 推出 ϕ 是一个满同态, 并且 $|\operatorname{Ker}\phi| = q$. 由此可知, 对于任意给定的元素 $a \in \mathbb{F}_q$, 有且恰有 q 个 $x \in \mathbb{F}_{q^2}$ 使得 $x + \overline{x} = a$.

类似地, 考虑从 $\mathbb{F}_{q^2}$ 的乘法群 $\mathbb{F}_{q^2}^*$ 到 $\mathbb{F}_q$ 的乘法群 $\mathbb{F}_q^*$ 的如下映射:

$$\begin{aligned} \psi : \mathbb{F}_{q^2}^* &\longrightarrow \mathbb{F}_q^* \\ x &\longmapsto x\overline{x}, \end{aligned}$$

容易推出 $\operatorname{Ker}|\psi| = q + 1$, $|\operatorname{Im}\psi| = q - 1$. 于是对于任意给定的元素 $a \in \mathbb{F}_q^*$, 有且恰有 $q + 1$ 个元素 $x \in \mathbb{F}_{q^2}^*$ 使得 $x\overline{x} = a$. 这样, 我们证明了

引理 4.1　对于任意元素 $a \in \mathbb{F}_q$, 有且恰有 q 个元素 $x \in \mathbb{F}_{q^2}$, 使得 $x + \overline{x} = a$. 对于任意元素 $a \in \mathbb{F}_q^*$, 有且恰有 $q + 1$ 个元素 $x \in \mathbb{F}_q^*$, 使得 $x\overline{x} = a$.

设 n 为一正整数. $\mathbb{F}_{q^2}$ 上的 $n \times n$ 矩阵 $A = (a_{ij})$ 叫做Hermite 矩阵, 如果对于任意一对 i, j 有 $a_{ji} = \overline{a}_{ij}$. 显然, A 的主对角线上的元素 a_{ii} 均属于 $\mathbb{F}_q$. 对于 $\mathbb{F}_{q^2}$ 上任意 $n \times n$ 矩阵 $X = (x_{ij})$, 记 $\overline{X} = (\overline{x}_{ij})$. 再记 ${}^tX$ 为 X 的转置, 那么 X 是 Hermite 矩阵如果 ${}^t\overline{X} = X$.

现在, 令 $\mathcal{H}(n, q^2)$ 表示 $\mathbb{F}_{q^2}$ 上全体 $n \times n$ Hermite 矩阵的集合. 显然, $\mathcal{H}(n, q^2)$ 对于矩阵加法做成一个加法群, 它的阶为 $|\mathcal{H}(n, q^2)| = q^{n^2}$. $\mathbb{F}_{q^2}$ 上的一般线性群 $GL_n(\mathbb{F}_{q^2})$ 如下作用在 $\mathcal{H}(n, q^2)$ 上:

$$\begin{aligned} GL_n(\mathbb{F}_{q^2}) \times \mathcal{H}(n, q^2) &\longrightarrow \mathcal{H}(n, q^2) \\ (T, X) &\longmapsto TX\,{}^t\overline{T}. \end{aligned} \tag{4.1}$$

这样每个 $T \in GL_n(\mathbb{F}_{q^2})$ 给出加法群 $\mathcal{H}(n, q^2)$ 的一个自同构. 令 T_0 表示加法群 $\mathcal{H}(n, q^2)$ 的平移群, 并令 G 是由 $GL_n(\mathbb{F}_{q^2})$ 和 T_0 生成的群, 它是 $\mathcal{H}(n, q^2)$ 上的一个置换群. 具体地说, G 的元素 $(T, A)(T \in GL_n(\mathbb{F}_{q^2}), A \in \mathcal{H}(n, q^2))$ 将 $\mathcal{H}(n, q^2)$ 的元素 X 映到

$$X \longmapsto TX\,{}^t\overline{T} + A. \tag{4.2}$$

群 G 的作用 (4.2) 是可迁的, 于是由定理 1.4 知, $(G, \mathcal{H}(n, q^2))$ 确定了 $\mathcal{H}(n, q^2)$ 上的一个结合方案, 叫做 $\mathbb{F}_{q^2}$ 上 n 阶Hermite 矩阵的结合方案, 记作 $\mathrm{Her}(n, q^2)$.

这个方案的类数等于在 $GL_n(\mathbb{F}_{q^2})$ 的作用 (4.1) 之下 $\mathcal{H}(n, q^2)$ 的非平凡轨道数. $\mathcal{H}(n, q^2)$ 中的两个矩阵 X 和 Y 在同一个 $GL_n(\mathbb{F}_{q^2})$ 轨道, 当且仅当存在矩阵 $T \in GL_n(\mathbb{F}_{q^2})$ 使得 $Y = TX\,{}^t\overline{T}$. 由 [15] 的定理 5.2 知, 如果 Hermite 矩阵 H 的秩为 $r\,(0 \leqslant r \leqslant n)$, 那么存在 $T \in GL_n(\mathbb{F}_{q^2})$ 使得

$$TH\,{}^t\overline{T} = [I^{(r)}, 0^{(n-r)}]. \tag{4.3}$$

这样, 两个 $n \times n$ Hermite 矩阵 X 和 Y 在同一个 $GL_n(\mathbb{F}_{q^2})$ 轨道, 当且仅当它们有相同的秩. 于是结合方案 $\mathrm{Her}(n, q^2)$ 的类数为 n. 令

$$C_i = \{X \in \mathcal{H}(n, q^2) | \mathrm{rank}\, X = i\},\ i = 0, 1, \cdots, n.$$

那么, 对应的结合类

$$R_i = \{(X, Y) | Y - X \in C_i\},\ 0 \leqslant i \leqslant n.$$

易见每个 R_i 都是对称的, 因而结合方案 $\mathrm{Her}(n, q^2)$ 是对称的.

现在, 我们讨论结合方案 $\mathrm{Her}(n, q^2)$ 的本原性. 我们先证明下面的

定理 4.2 群 $G = GL_n(\mathbb{F}_{q^2}) \cdot T_0$ 作用在 $\mathcal{H}(n, q^2)$ 上是本原的.

证明 从 G 在 $\mathcal{H}(n, q^2)$ 上的作用 (4.2) 知, G 的两个元素 (T_1, A_1) 和 (T_2, A_2) 的乘积为

$$(T_1, A_1)(T_2, A_2) = (T_2T_1, T_2A_1\,{}^t\overline{T_2} + A_2). \tag{4.4}$$

$\mathcal{H}(n, q^2)$ 中的零矩阵 0 的稳定子 $G_0 = \{(T, 0) | T \in GL_n(\mathbb{F}_{q^2})\}$. 往证: G_0 是 G 的一个极大子群.

设 N 为 G 的一个子群使得 $G_0 \subsetneq N$. 于是存在元素 $(P, A) \in N$ 而且 $A \neq 0$. 再由于 $G_0 \subset N$, 所以

$$(P^{-1}, 0)(P, A) = (I, A) \in N. \tag{4.5}$$

令

$$W = \{X \in \{\mathcal{H}(n, q^2) | (I, X) \in N\},$$

由 (4.5) 知 $W \neq \{0\}$. 由于

$$(I,\, X)(I,\, Y) = (I,\, X+Y)$$

可知 W 对于矩阵加法是封闭的. 进一步, 由 (4.5) 知, $A \in W$. 设 $\operatorname{rank} A = r$, 那么, 从

$$(T^{-1},\, 0)(I,\, A)(T,\, 0) = (I,\, TA\,{}^t\overline{T}) \in N$$

推出 $C_r \subset W$. 如果 $r \geqslant 2$, 由于

$$[I^{(r)},\, 0^{(n-1)}] + \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\, -I^{(r-2)},\, 0^{(n-r)}\right] = \left[\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix},\, 0^{(n-2)}\right] \in W,$$

可知 $C_1 \subset W$. 由 (4.3) 可知, 每个非零 Hermite 矩阵均可表示成若干秩为 1 的 Hermite 矩阵之和, 于是 $W = \mathcal{H}(n,\, q^2)$, 因而推出 $N = G$. 定理得证. □

由定理 4.2 和定理 1.18 我们就有

定理 4.3　Hermite 矩阵的结合方案 $\mathrm{Her}(n,\, q^2)$ 是本原的, 因而它的结合关系图 $\Gamma^{(i)}\,(i = 1,\, 2,\, \cdots,\, n)$ 都是连通的.

由于 Hermite 矩阵有形如 (4.3) 的合同标准形, 类似于定理 2.5 和定理 2.6, 我们有

定理 4.4　Hermite 矩阵结合方案 $\mathrm{Her}(n,\, q^2)$ 的结合关系图 $\Gamma^{(1)}$ 是距离可迁的, 因而它是距离正则的.

图 $\Gamma^{(1)}$ 中距离为 i 的顶点对子 $(X,\, Y)$ 恰好组成结合方案 $\mathrm{Her}(n,\, q^2)$ 的结合关系 $R_i\,(i = 0,\, 1,\, \cdots,\, n)$. 因此, 我们有

定理 4.5　$\mathbb{F}_{q^2}$ 上 $n \times n$ Hermite 矩阵的结合方案 $\mathrm{Her}(n,\, q^2)$ 在顺序 $R_0,\, R_1,\, \cdots,\, R_n$ 之下是 P 多项式的.

文献中把结合关系图 $\Gamma^{(1)}$ 叫做 $n \times n$ Hermite 矩阵的图, 记作 $\mathrm{Her}(n,\, q^2)$. 由于这个图完全决定了 Hermite 矩阵的结合方案, 所以我们把这个结合方案也记作 $\mathrm{Her}(n,\, q^2)$.

§4.2　关系图 $\Gamma^{(1)}$ 的参数

关于结合方案 $\mathrm{Her}(n,\, q^2)$ 的参数 p_{ij}^k 的计算, 我们要用到 [15] 中有关酉几何的两个计数公式.

设 n 为正整数. H 为 $\mathbb{F}_{q^2}$ 上的一个 $n \times n$ 非奇异 Hermite 矩阵, 如果矩阵 $T \in GL_n(\mathbb{F}_{q^2})$ 满足条件

$$TH\,{}^t\overline{T} = H, \tag{4.6}$$

则称它是一个关于 H 的U 矩阵. 关于 H 的全体 U 矩阵作成 $GL_n(\mathbb{F}_{q^2})$ 的一个子群, 叫做 $\mathbb{F}_{q^2}$ 上关于 H 的 n 级U 群, 记作 $U_n(H, \mathbb{F}_{q^2})$. 容易证明, 如果 H_1 和 H_2 是 $\mathbb{F}_{q^2}$ 上两个 $n\times n$ 非奇异 Hermite 矩阵, 那么 U 群 $U_n(H_1, \mathbb{F}_{q^2})$ 和 $U_n(H_2, \mathbb{F}_{q^2})$ 是同构的. 因此, 我们可取 (4.6) 中的 $H=I^{(n)}$. 这时, 关于 $I^{(n)}$ 的 U 矩阵 T 满足

$$T\,{}^t\overline{T}=I^{(n)}.$$

简称为U 矩阵, 相应的U 群简记为 $U_n(\mathbb{F}_{q^2})$. 由 [15] 中定理 5.6 知, U 群 $U_n(\mathbb{F}_{q^2})$ 的阶为

$$|U_n(\mathbb{F}_{q^2})|=q^{\frac{1}{2}n(n-1)}\prod_{j=1}^{n}(q^j-(-1)^j). \tag{4.7}$$

$U_n(\mathbb{F}_{q^2})$ 自然地如下作用在 $\mathbb{F}_{q^2}^{(n)}$ 上:

$$\begin{aligned}\mathbb{F}_{q^2}^{(n)}\times U_n(\mathbb{F}_{q^2}) &\longrightarrow \mathbb{F}_{q^2}^{(n)}\\ ((x_1,\cdots,x_n),T) &\longmapsto (x_1,\cdots,x_n)T.\end{aligned}$$

向量空间 $\mathbb{F}_{q^2}^{(n)}$ 连同 U 群 $U_n(\mathbb{F}_{q^2})$ 的作用称为 U 空间. U 矩阵 T 自然地作用在 $\mathbb{F}_{q^2}^{(n)}$ 的子空间的集合上.

设 P 是 $\mathbb{F}_{q^2}^{(n)}$ 的一个 m 维子空间, 和前面一样, 我们仍用 P 作为它的一个矩阵表示, 即 P 是以子空间 P 的一组基向量为行作成的秩为 m 的 $m\times n$ 矩阵. 说子空间 P (关于 $H=I^{(n)}$) 是(m, r) 型的, 如果 $\operatorname{rank} P\,{}^t\overline{P}=r$, 这里 m, r 满足条件 $2r\leqslant 2m\leqslant n+r$. $(m, 0)$ 型子空间称为 m 维全迷向子空间. (m, m) 型子空间称为 m 维非迷向子空间. 下面的 $m\times n$ 矩阵

$$\begin{pmatrix} I^{(r)} & 0 & 0 & 0\\ 0 & I^{(m-r)} & \lambda I^{(m-r)} & 0\end{pmatrix}\begin{matrix}\\ \\ \end{matrix} \tag{4.8}$$
$$\qquad r \qquad m-r \qquad m-r \qquad n-2m-r$$

就是一个 (m, r) 型子空间, 这里 $\lambda\overline{\lambda}=-1$.

在 U 群 $U_n(\mathbb{F}_{q^2})$ 作用下, $\mathbb{F}_{q^2}^{(n)}$ 中类型相同的子空间组成一个轨道 [15]. 令 $N(m, r; n)$ 表示 $\mathbb{F}_{q^2}^{(n)}$ 中全体 (m, r) 型子空间的个数, 由 [15] 中定理 5.19 知

$$N(m, r; n)=q^{r(n+r-2m)}\frac{\displaystyle\prod_{j=n+r-2m+1}^{n}(q^j-(-1)^j)}{\displaystyle\prod_{j=1}^{r}(q^j-(-1)^j)\prod_{j=1}^{m-r}(q^{2j}-1)}. \tag{4.9}$$

在下面的参数计算中, 我们将用到关于矩阵的一个计数公式. 设 A 是 $\mathbb{F}_{q^2}$ 上的一个 $l\times n$ 矩阵, 如果 $\operatorname{rank} A=m$ 并且 $\operatorname{rank} A\,{}^t\overline{A}=r$, 那么称 A 是 (关于 $H=I^{(n)}$) 的一个(m, r) 型矩阵, 这里 $2r\leqslant 2m\leqslant n+r$. 令 $n(l\times n; m, r)$ 表示 $\mathbb{F}_{q^2}$ 上全体 (关于 $H=I^{(n)}$) 型为 (m, r) 的 $l\times n$ 矩阵之个数, 我们有

定理 4.6 设 $m \leqslant l$ 且 $2r \leqslant 2m \leqslant n+r$. $\mathbb{F}_{q^2}$ 上 (关于 $H = I^{(n)}$) 型为 (m, r) 的 $l \times n$ 矩阵之个数

$$n(l \times n;\, m,\, r) = q^{r(n+r-2m)+m(m-1)} \cdot \frac{\prod_{j=n+r-2m+1}^{n} (q^j - (-1)^j) \prod_{j=l-m+1}^{l} (q^{2j} - 1)}{\prod_{j=1}^{r} (q^j - (-1)^j) \prod_{j=1}^{m-r} (q^{2j} - 1)}. \tag{4.10}$$

证明 对于 $\mathbb{F}_{q^2}^{(n)}$ 中每个 (m, r) 型子空间 P 取定它的一个矩阵表示, 仍记为 P. 那么 $\mathbb{F}_{q^2}$ 上 $l \times n$ 矩阵 Q 的行向量生成子空间 P, 当且仅当 $Q = AP$, 这里 A 为 $\mathbb{F}_{q^2}$ 上的一个秩为 m 的 $l \times m$ 矩阵. 于是 $n(l \times n;\, m,\, r) = n_m(l \times m,\, q) \cdot N(m,\, r;\, n)$. 由 (4.9) 和定理 2.1 立得 (4.10). □

现在我们回到 Hermite 矩阵结合方案的参数计算.Her(n, q^2) 的结合关系 R_i 的价 $k_i = |C_i|$. 令 $H_i(n, q^2) = |C_i|$, 即 $\mathbb{F}_{q^2}$ 上秩为 i 的 $n \times n$ Hermite 矩阵的个数, 我们有

定理 4.7 设 $0 \leqslant i \leqslant n$. $\mathbb{F}_{q^2}$ 上秩为 i 的 $n \times n$ Hermite 矩阵的个数为

$$H_i(n, q^2) = q^{\frac{1}{2}i(i-1)} \frac{\prod_{j=n-i+1}^{n} (q^{2j} - 1)}{\prod_{j=1}^{i} (q^j - (-1)^j)}. \tag{4.11}$$

证明 在 $GL_n(\mathbb{F}_{q^2})$ 的作用 (4.1) 之下, C_i 为一轨道. 取 C_i 的一个元素

$$H_i = [I^{(i)},\, 0^{(n-i)}].$$

H_i 在 $GL_n(\mathbb{F}_{q^2})$ 中的稳定子 G_{H_i} 由满足条件 $TH_i{}^t\overline{T} = H_i$ 的矩阵 T 组成. 将 T 相应于 H_i 分块

$$T = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{matrix} i \\ n-i \end{matrix}, \quad \text{列分块: } i,\ n-i$$

于是有下面的等式

$$A\,{}^t\overline{A} = I^{(i)}, \quad C\,{}^t\overline{A} = 0.$$

由此可知 $A \in U_i(\mathbb{F}_{q^2})$, 特别是, A 非奇异, 因而 $C = 0$, $D \in GL_{n-i}(\mathbb{F}_{q^2})$. 这样

$$|G_{H_i}| = |U_i(\mathbb{F}_{q^2})||GL_{n-i}(\mathbb{F}_{q^2})|q^{2i(n-i)}.$$

由 (4.7) 和 (2.2) 即可得 (4.11). □

下面我们计算结合方案 $\mathrm{Her}(n,q^2)$ 的关系图 $\Gamma^{(1)}$ 的参数. 由定理 4.7 知, $\Gamma^{(1)}$ 的价

$$k_1 = H_1(n,\,q^2) = \frac{q^{2n}-1}{q+1}.$$

由定理 4.4, $\Gamma^{(1)}$ 是距离正则的. 我们先计算它的参数 $c_i = p^i_{1i-1}$, $a_i = p^i_{1i}$ 和 $b_i = p^i_{1i+1}$. 不失一般性, 我们可以取

$$A = [I^{(i)},\, 0^{(n-i)}].$$

设 X 是秩为 1 的 Hermite 矩阵, 观察 $A-X$ 的秩. 因为 $\mathrm{rank}\,X=1$, 从 (4.3) 可知, 存在 $\mathbb{F}_{q^2}^{(n)}$ 中的向量 $u\neq 0$ 使得 $X = {}^t\overline{u}u$, 并且如果 $v\in\mathbb{F}_{q^2}^{(n)}$ 也有 $X={}^t\overline{v}v$, 当且仅当有 $\alpha\in\mathbb{F}_{q^2}^*$ 使 $v=\alpha u$ 且 $\alpha\overline{\alpha}=1$. 现在设

$$u=(u_1,\,u_2),\ u_1=(x_1,\,\cdots,\,x_i),\ u_2=(x_{i+1},\,\cdots,\,x_n).$$

于是

$$A-X=\left(\begin{array}{c|c} I^{(i)}-{}^t\overline{u}_1\,u_1 & -{}^t\overline{u}_1\,u_2 \\ \hline -{}^t\overline{u}_2u_1 & -{}^t\overline{u}_2u_2\end{array}\right).$$

如果 $u_2\neq 0$, 则存在 $T_1\in GL_{n-i}(\mathbb{F}_{q^2})$ 使 $u_2T_1=(1,\,0,\,\cdots,\,0)$. 这时令 $T=I^{(i)}+T_1$, 那么

$${}^t\overline{T}(A-X)T=\left(\begin{array}{c|cc} I^{(i)}-{}^t\overline{u}_1u_1 & -{}^t\overline{u}_1 & 0 \\ \hline -u_1 & -1 & \\ 0 & & 0\end{array}\right).$$

这时 $\mathrm{rank}\,(A-X)=i+1$. 这种 X 的个数为 $q^{2i}(q^{2(n-i)}-1)/(q+1)$.

如果 $u_2=0$, 那么 $u_1\neq 0$. 这时 $X=[{}^t\overline{u}_1u_1,\,0]$, 因此只需考虑 $I^{(i)}-{}^t\overline{u}_1u_1$. 由于 $\mathrm{rank}\,({}^t\overline{u}_1u_1)=1$, 所以 $\mathrm{rank}\,(I^{(i)}-{}^t\overline{u_1}u_1)=i-1$ 或 i. 计算

$$\begin{aligned}\det(I^{(i)}-{}^t\overline{u}_1u_1) &= \det\begin{pmatrix}1-\overline{x}_1x_1 & -\overline{x}_1x_2 & \cdots & -\overline{x}_1x_i\\ -\overline{x}_2x_1 & 1-\overline{x}_2x_2 & \cdots & -\overline{x}_2x_i\\ \vdots & \vdots & & \vdots\\ -\overline{x}_ix_1 & -\overline{x}_ix_2 & \cdots & 1-\overline{x}_ix_i\end{pmatrix}\\ &= 1-\overline{x}_1x_1-\cdots-\overline{x}_ix_i\end{aligned}$$

可知,

$$\mathrm{rank}\,(I^{(i)}-{}^t\overline{u}_1u_1)=\begin{cases} i-1, & \text{如果}\,\overline{x}_1x_1+\cdots+\overline{x}_ix_i=1,\\ i, & \text{如果}\,\overline{x}_1x_1+\cdots+\overline{x}_ix_i\neq 1.\end{cases}$$

由定理 4.6 可知, 使 $\overline{x}_1x_1+\cdots+\overline{x}_ix_i=1$ 的向量 $u_1=(x_1,\,\cdots,\,x_i)$ 的个数为

$$\frac{n(1\times i;\,1,\,1)}{q-1}=\frac{q^{i-1}(q^i-(-1)^i)(q^2-1)}{(q-1)(q+1)}=q^{i-1}(q^i-(-1)^i).$$

于是使 $\operatorname{rank}(I^{(i)} - {}^t\overline{u}_1 u_1) = i-1$ 的矩阵 ${}^t\overline{u}_1 u_1$ 的个数为 $q^{i-1}(q^i - (-1)^i)/(q+1)$. 这样我们有

定理 4.8　结合方案 $\mathrm{Her}(n, q^2)$ 的关系图 $\Gamma^{(1)}$ 的参数为

$$\begin{aligned} b_i =& p^i_{1i+1} = \frac{q^{2i}(q^{2(n-i)}-1)}{q+1}, \ 0 \leqslant i < n. \\ c_i =& p^i_{1i-1} = \frac{q^{i-1}(q^i-(-1)^i)}{q+1}, \ 0 < i \leqslant n. \\ a_i =& p^i_{1i} = \frac{q^{2i}-q^{i-1}(q^i-(-1)^i)-1}{q+1}, \ 0 < i \leqslant n. \end{aligned}$$

§4.3　交叉数 p^k_{ij} 的递推计算

对于结合方案 $\mathrm{Her}(n, q^2)$ 的交叉数 p^k_{ij}, 我们给出它们的递推计算公式. 为此把这些交叉数记作 $p^k_{ij}(n)$. 我们有

定理 4.9　设 $0 < k < n$. $\mathrm{Her}(n, q^2)$ 的交叉数

$$p^k_{ij}(n) = \sum_{\substack{0 \leqslant \alpha \leqslant \min\{i, n-k\} \\ 0 \leqslant \gamma \leqslant \beta \leqslant \min\{k,\, n-k-\alpha\} \\ \alpha+2\beta \leqslant \min\{i,j\} \\ 2\beta \leqslant k+\gamma}} H_\alpha(n-k, q^2) n((n-k-\alpha)\times k;\, \beta,\, \gamma) \cdot q^{2k(\alpha+\beta)-\beta^2} p^{k+\gamma-2\beta}_{i-\alpha-2\beta, j-\alpha-2\beta}(k-\beta). \tag{4.12}$$

证明　设

$$A = [I^{(k)},\ 0^{(n-k)}].$$

令

$$\mathcal{M}^k_{ij} = \{H \in \mathcal{H}(n,\, q^2) | \operatorname{rank} H = i,\ \operatorname{rank}(H - A) = j\}.$$

于是 $p^k_{ij}(n) = |\mathcal{M}^k_{ij}|$. 对于任意 $H \in \mathcal{M}^k_{ij}$, 做相应于 A 的分块

$$H = \begin{pmatrix} U & V \\ {}^t\overline{V} & W \end{pmatrix} \begin{matrix} k \\ n-k \end{matrix}, \quad {}^t\overline{U} = U,\ {}^t\overline{W} = W. \tag{4.13}$$
$$\qquad\quad k \qquad n-k$$

我们按 H 的右下角块 W 的秩将 $\mathcal{M}^k_{ij}$ 的元素分组. 对于 $0 \leqslant \alpha \leqslant n-k$, 令

$$\mathcal{M}(\alpha) = \{H \in \mathcal{M}^k_{ij} | \operatorname{rank} W = \alpha\}.$$

那么有

$$|\mathcal{M}^k_{ij}| = \sum_{0 \leqslant \alpha \leqslant n-k} |\mathcal{M}(\alpha)|. \tag{4.14}$$

(α 满足进一步的条件将在下面给出.) 设 $\mathcal{M}(\alpha) \neq \varnothing$, 任取其中一个元素 H, 设有形状 (4.13). 由于 $\operatorname{rank} W = \alpha$, 所以存在 $P \in GL_{n-k}(\mathbb{F}_{q^2})$, 使得

$$PW\,{}^t\overline{P} = [I^{(\alpha)}, 0^{(n-k-\alpha)}].$$

令 $T = I^{(k)} \dot{+} P$, 那么 T 导出的合同变换, 使 A 不动, 而将 H 变到

$$PH\,{}^t\overline{P} = \begin{pmatrix} U & V\,{}^t\overline{P} \\ P\,{}^t\overline{V} & PW\,{}^t\overline{P} \end{pmatrix},$$

并将 $\mathcal{M}(\alpha)$ 变到自身, 令 $\mathcal{M}_1$ 为 $\mathcal{M}(\alpha)$ 中全体形如

$$\left(\begin{array}{c|cc} U & V_1 & V_2 \\ \hline {}^t\overline{V_1} & I^{(\alpha)} & 0 \\ {}^t\overline{V_2} & 0 & 0 \end{array}\right) \begin{matrix} k \\ \alpha \\ n-k-\alpha \end{matrix} \tag{4.15}$$

的元素所成的集合, 于是我们有

$$|\mathcal{M}(\alpha)| = H_\alpha(n-k, q^2)|\mathcal{M}_1|. \tag{4.16}$$

现在, 施行由

$$T = \left[\begin{pmatrix} I^{(k)} & -V_1 \\ 0 & I^{(\alpha)} \end{pmatrix}, I^{(n-k-\alpha)}\right]$$

导出的变换, 将矩阵 (4.15) 变到

$$\begin{pmatrix} U^* & 0 & V \\ 0 & I^{(\alpha)} & 0 \\ {}^t\overline{V} & 0 & 0 \end{pmatrix} \begin{matrix} k \\ \alpha \\ n-k-\alpha \end{matrix} \tag{4.17}$$

而使 A 不动, 同时将 $\mathcal{M}_1$ 变到 $\mathcal{M}_1$. 我们令 $\mathcal{M}_2$ 为 $\mathcal{M}_1$ 中全体形如 (4.17) 的元素所成的集合, 于是有

$$|\mathcal{M}_1| = q^{2k\alpha}|\mathcal{M}_2|. \tag{4.18}$$

我们将 $\mathcal{M}_2$ 中的元素按形状 (4.17) 中左下角块 ${}^t\overline{V}$ 的类型来分组, 其中 ${}^t\overline{V}$ 是一个 $(n-k-\alpha) \times k$ 矩阵. 令 $\mathcal{M}(\beta, \gamma)$ 是 $\mathcal{M}_2$ 中左下角块 ${}^t\overline{V}$ 关于 $I^{(k)}$ 是 (β, γ) 型矩阵的那些元素的集合, 于是

$$|\mathcal{M}_2| = \sum_{\substack{0 \leqslant \gamma \leqslant \beta \leqslant \min\{n-k-\alpha, k\} \\ 2\beta \leqslant k+\gamma}} |\mathcal{M}(\beta, \gamma)|. \tag{4.19}$$

设 $\mathcal{M}(\beta, \gamma) \neq \varnothing$. 又设

$$H = \begin{pmatrix} U & 0 & V \\ 0 & I^{(\alpha)} & 0 \\ {}^t\overline{V} & 0 & 0 \end{pmatrix} \in \mathcal{M}(\beta, \gamma), \tag{4.20}$$

其中 ${}^t\overline{V}$ 关于 $I^{(k)}$ 是 (β,γ) 型的. 那么由 (4.8) 可知, 存在 $Q\in GL_{n-k-\alpha}(\mathbb{F}_{q^2})$ 及 ${}^t\overline{T}_1\in U_k(\mathbb{F}_{q^2})$, 使得

$$Q\,{}^t\overline{V}\,{}^t\overline{T}_1=\begin{pmatrix} I^{(\gamma)} & 0 & 0 & 0\\ 0 & I^{(\beta-\gamma)} & \overline{\lambda}I^{(\beta-\gamma)} & 0\\ 0 & 0 & 0 & 0 \end{pmatrix}\begin{matrix}\gamma\\ \beta-\gamma\\ n-k-\alpha-\beta\end{matrix}, \quad \lambda\overline{\lambda}=-1. \tag{4.21}$$
$$\qquad\qquad\qquad \gamma \qquad\quad \beta-\gamma \qquad \beta-\gamma \qquad k+\gamma-2\beta$$

令 $T=[T_1,\,I^{(\alpha)},\,Q]$, 那么由 T 导出的合同变换使 A 不动, 将 $\mathcal{M}(\beta,\,\gamma)$ 映到自身, 而将矩阵 (4.20) 变到 $TH\,{}^t\overline{T}$, 其左下角块有形状 (4.21). 令 $\mathcal{M}_3$ 为 $\mathcal{M}(\beta,\,\gamma)$ 中左下角块有形状 (4.21) 的那些矩阵所成的集合. 于是可知

$$|\mathcal{M}(\beta,\,\gamma)|=n((n-k-\alpha)\times k;\,\beta,\,\gamma)|\mathcal{M}_3|. \tag{4.22}$$

设 $H\in\mathcal{M}_3$, 那么它有如下形状

$$H=\left(\begin{array}{cccc|c|ccc} U_{11} & U_{12} & U_{13} & U_{14} & & I^{(\gamma)} & 0 & 0\\ {}^t\overline{U}_{12} & U_{22} & U_{23} & U_{24} & 0 & 0 & I^{(\beta-\gamma)} & 0\\ {}^t\overline{U}_{13} & {}^t\overline{U}_{23} & U_{33} & U_{34} & & 0 & \lambda I^{(\beta-\gamma)} & 0\\ {}^t\overline{U}_{14} & {}^t\overline{U}_{24} & {}^t\overline{U}_{34} & U_{44} & & 0 & 0 & 0\\ \hline & & 0 & & I^{(\alpha)} & & 0 & \\ \hline I^{(\gamma)} & 0 & 0 & 0 & & & & \\ 0 & I^{(\beta-\gamma)} & \overline{\lambda}I^{(\beta-\gamma)} & 0 & 0 & & 0 & \\ 0 & 0 & 0 & 0 & & & & \end{array}\right)\ k+\gamma-2\beta\ .$$

对 H 施行适当的变换可化为形如

$$\left(\begin{array}{cccc|c|ccc} 0 & 0 & 0 & 0 & & I^{(\gamma)} & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & I^{(\beta-\gamma)} & 0\\ 0 & 0 & U_1 & U_2 & & 0 & \lambda I^{(\beta-\gamma)} & 0\\ 0 & 0 & {}^t\overline{U}_2 & U_3 & & 0 & 0 & 0\\ \hline & & 0 & & I^{(\alpha)} & & 0 & \\ \hline I^{(\gamma)} & 0 & 0 & 0 & & & & \\ 0 & I^{(\beta-\gamma)} & \overline{\lambda}I^{(\beta-\gamma)} & 0 & 0 & & 0 & \\ 0 & 0 & 0 & 0 & & & & \end{array}\right)\ k+\gamma-2\beta\ . \tag{4.23}$$

令 $\mathcal{M}_4$ 为 $\mathcal{M}_3$ 中全体形如 (4.23) 的矩阵所成的集合, 那么有

$$|\mathcal{M}_3|=q^{2k\beta-\beta^2}|\mathcal{M}_4|. \tag{4.24}$$

设 $H\in\mathcal{M}_4$. 由 $\operatorname{rank}H=i$ 知

$$\operatorname{rank}\begin{pmatrix} U_1 & U_2\\ {}^t\overline{U}_2 & U_3\end{pmatrix}=i-\alpha-2\beta. \tag{4.25}$$

再由 $\operatorname{rank}(H-A)=j$, 简单计算即可知

$$\operatorname{rank}\left[\begin{pmatrix} U_1 & U_2 \\ {}^t\overline{U}_2 & U_3 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 0 & I \end{pmatrix}\right] = j-\alpha-2\beta. \tag{4.26}$$

因此, 由 (4.25) 和 (4.26) 可知

$$|\mathcal{M}_4| = p^{k+\gamma-2\beta}_{i-\alpha-2\beta,j-\alpha-2\beta}(k-\beta). \tag{4.27}$$

于是由 (4.14), (4.16), (4.18), (4.19),(4.22), (4.24) 和 (4.27) 即得 (4.12). 定理得证.□

§4.4 交叉数计算续

现在, 我们给出交叉数 $p^n_{nn}(n)$ 的一个降阶递推计算公式. 首先观察一个 n 阶满秩 Hermite 矩阵 X 怎样从一个 $n-1$ 阶主子矩阵扩充而来?

写 X 为如下形状

$$X = \begin{pmatrix} Y & u \\ {}^t\overline{u} & w \end{pmatrix} \begin{matrix} n-1 \\ 1 \end{matrix}, \qquad \begin{matrix} n-1 & 1 \end{matrix} \tag{4.28}$$

并设 $\operatorname{rank}X=n$. 我们断言: $\operatorname{rank}Y=n-1$ 或 $n-2$. 实际上, 设 $\operatorname{rank}Y=r$, 那么存在 $T\in GL_{n-1}(\mathbb{F}_{q^2})$, 使得 $TY\,{}^t\overline{T}=I^{(r)}\dot{+}0^{(n-r-1)}$. 令 $P=T\dot{+}(1)$. 于是

$$PX\,{}^t\overline{P} = \begin{pmatrix} I^{(r)} & 0 & v_1 \\ 0 & 0 & v_2 \\ {}^t\overline{v}_1 & {}^t\overline{v}_2 & w \end{pmatrix} \text{ 合同于 } \begin{pmatrix} I^{(r)} & 0 & 0 \\ 0 & 0 & v_2 \\ 0 & {}^t\overline{v}_2 & w^* \end{pmatrix},$$

这里 ${}^t\overline{u}\,{}^t\overline{P}=({}^t\overline{v}_1,\ {}^t\overline{v}_2)$, $w^*=w-{}^t\overline{v}_1v_1$. 由此可知 $r=n-1$ 或 $n-2$. 如果 $r=n-1$, 那么 v_2 不出现, 这时对于任意 ${}^t\overline{v}\in\mathbb{F}_{q^2}^{(n-1)}$ 及 $w\in\mathbb{F}_q$, 使得 $w\neq{}^t\overline{v}v$ 者均有形如 (4.28) 的扩充 X, 使得 $\operatorname{rank}X=n$. 如果 $r=n-2$, 那么对于任意 ${}^t\overline{v}_1\in\mathbb{F}_q^{(n-2)}$ 和 $v_2\in\mathbb{F}_{q^2}^*$ 以及任意 $w\in\mathbb{F}_q$, 均有形如 (4.28) 的扩充 X 使得 $\operatorname{rank}X=n$. 每个满秩 n 阶 Hermite 矩阵均可如上扩充得到. 当 $\operatorname{rank}Y=n-1$ 时, 有 $q^{2(n-1)}(q-1)$ 个形如 (4.28) 的满秩 Hermite 矩阵 X. 当 $\operatorname{rank}Y=n-2$ 时, 有 $q^{2(n-2)}(q^2-1)q$ 个形如 (4.28) 的满秩 Hermite 矩阵 X.

令 H 为如下形状的 n 阶 Hermite 矩阵

$$H = \begin{pmatrix} I^{(n-1)} & v \\ {}^t\overline{v} & x \end{pmatrix}, \tag{4.29}$$

这里 $v={}^t(x_1,\cdots,x_{n-1})$. 再令 $\mathcal{Y}$ 为如下 n 阶 Hermite 矩阵对子所成集合:

$$\mathcal{Y}=\{(H,X)|H\text{形如 (4.29)}, \operatorname{rank}X=n, \operatorname{rank}\ (X+H)=n\}.$$

我们用两种方法来计算 $|Y|$.

第一种方法是先取 H 然后再取 X. 当 $x \neq {}^t\overline{v}v$ 时, $\operatorname{rank} H = n$. 这时 X 有 $p^n_{n\,n}(n)$ 个选取, 这种对子 (H, X) 的个数为 $q^{2(n-1)}(q-1)p^n_{nn}(n)$. 当 $x = {}^t\overline{v}v$ 时, $\operatorname{rank} H = n-1$. 这时 X 有 $p^{n-1}_{n\,n}(n)$ 个选取, 这种对子 (H, X) 的个数为 $q^{2(n-1)}p^{n-1}_{nn}(n)$. 因此

$$|Y| = q^{2(n-1)}(q-1)p^n_{nn}(n) + q^{2(n-1)}p^{n-1}_{n\,n}(n). \tag{4.30}$$

第二种方法是先取 X, 然后取 H. 考虑 X 有形状 (4.28), 它的左上角 $n-1$ 阶子矩阵 Y 的秩或为 $n-1$ 或为 n. 因为要求 $\operatorname{rank}(X+H) = n$, 所以 $\operatorname{rank}(Y+I^{(n-1)}) = n-1$ 或 $n-2$. 这样 Y 有下面 4 种可能:

(i) $\operatorname{rank} Y = n-1$, $\operatorname{rank}(Y+I^{(n-1)}) = n-1$. 这样的 Y 有 $p^{n-1}_{n-1n-1}(n-1)$ 个, 当 Y 取定后, 将它扩充成满秩的 X 有 $q^{2(n-1)}(q-1)$ 个. 再利用条件 $\operatorname{rank}(X+H) = n$ 可得到 $q^{2(n-1)}(q-1)$ 个 H. 这样有 $p^{n-1}_{n-1n-1}(n-1) \cdot q^{2(n-1)}(q-1) \cdot q^{2(n-1)}(q-1)$ 个对子 (H, X).

(ii) $\operatorname{rank} Y = n-1$, $\operatorname{rank}(Y+I^{(n-1)}) = n-2$. 类似地, 我们可得到

$$p^{n-1}_{n-1n-2}(n-1) \cdot q^{2(n-1)}(q-1) \cdot q^{2(n-2)}(q^2-1)q$$

个对子 (H, X).

(iii) $\operatorname{rank} Y = n-2$, $\operatorname{rank}(Y+I^{(n-1)}) = n-1$. 这种情形下可得到的对子个数为

$$p^{n-1}_{n-2\,n-1}(n-1) \cdot q^{2(n-2)}(q^2-1)q \cdot q^{2(n-1)}(q-1).$$

(iv) $\operatorname{rank} Y = n-2$, $\operatorname{rank}(Y+I^{(n-1)}) = n-2$. 这种情形下可得到的对子个数为

$$p^{n-1}_{n-2\,n-2}(n-1) \cdot q^{2(n-2)}(q^2-1)q \cdot q^{2(n-2)}(q^2-1)q.$$

于是我们得到

$$\begin{aligned} |Y| = &\ q^{4n-4}(q-1)^2 p^{n-1}_{n-1n-1}(n-1) + q^{4n-5}(q-1)(q^2-1) \cdot p^{n-1}_{n-1\,n-2}(n-1) \\ &+ q^{4n-5}(q-1)(q^2-1)p^{n-1}_{n-2\,n-1}(n-1) + q^{4n-6}(q^2-1)^2 p^{n-1}_{n-2\,n-2}(n-1). \end{aligned} \tag{4.31}$$

由 (4.30) 和 (4.31) 我们得到下面的公式

定理 4.10 对于任意正整数 n, 我们有

$$\begin{aligned} p^n_{nn}(n) =&\, q^{2n-2}(q-1)p^{n-1}_{n-1n-1}(n-1) + 2q^{2n-3}(q^2-1)p^{n-1}_{n-1\,n-2}(n-1) \\ &+ q^{2n-4}(q^2-1)(q+1)p^{n-1}_{n-2\,n-2}(n-1) - \frac{1}{q-1}p^{n-1}_{n\,n}(n). \end{aligned}$$

□

例 4.1 计算 $p_{22}^2(2)$.

$$\begin{aligned} p_{22}^2(2) &= q^2(q-1)p_{11}^1(1) + 2q(q^2-1)p_{10}^1(1) - \tfrac{1}{q-1}p_{22}^1(2) \\ &= q^2(q-1)(q-2) + 2q(q^2-1) - q(q^2-q+1) \\ &= q(q^3-2q^2+3q-3). \end{aligned}$$

例 4.2 利用公式 (4.12) 计算 $p_{33}^2(3)$.

$$\begin{aligned} p_{33}^2(3) = &\ H_1(1,q^2)\cdot q^4 \cdot p_{22}^2(2) \\ &+n(1\times 2;1,1)\cdot q^3\cdot p_{11}^1(1) + n(1\times 2;1,0)\cdot q^3 \cdot p_{11}^0(1) \\ = &\ q^4(q-1)p_{22}^2(2) + q^4(q^2-1)(q-1)(q-2) \\ &+q^3(q^2-1)(q+1)(q-1) \\ = &\ q^3(q-1)(q^5-q^4+2q^3-3q^2+q-1). \end{aligned}$$

§4.5 Hermite 矩阵结合方案的自对偶性

设 n 为正整数, $\mathcal{H}(n, q^2)$ 是域 $\mathbb{F}_{q^2}$ 上全体 $n\times n$ Hermite 矩阵对于矩阵加法作成的加法群,$\mathrm{Her}(n, q^2)$ 是 n 阶 Hermite 矩阵的结合方案. 在这一节中, 我们来证明结合方案 $\mathrm{Her}(n, q^2)$ 是自对偶的.

令 χ 是基域 $\mathbb{F}_{q^2}$ 的加法群 $(\mathbb{F}_{q^2}, +)$ 的一个非平凡复特征标. 对于每个 Hermite 矩阵 $A=(a_{ij})\in\mathcal{H}(n, q^2)(\overline{a}_{ij}=a_{ji})$, 我们定义一个映射

$$\begin{aligned} \phi_A : \mathcal{H}(n, q^2) &\longrightarrow \mathbb{C} \\ X=(x_{ij}) &\longmapsto \chi\left(\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_{ij}\right), \end{aligned} \tag{4.32}$$

这里 $\overline{x}_{ij}=x_{ji}$, 那么 ϕ_A 是 $\mathcal{H}(n, q^2)$ 的一个特征标, 并且有

$$\phi_{A+B} = \phi_A\phi_B.$$

命题 4.11 设 $A, B\in\mathcal{H}(n, q^2)$, 那么 $\phi_A=\phi_B$ 当且仅当 $A=B$. 于是映射 $A\mapsto\phi_A$ 是 $\mathcal{H}(n, q^2)$ 到它的特征标群 $\mathcal{H}(n, q^2)^*$ 的一个同构.

证明 略. □

命题 4.12 对于 $A, X\in\mathcal{H}(n,q^2)$ 及 $T\in GL_n(\mathbb{F}_{q^2})$, 恒有

$$\phi_A(TX\,{}^t\overline{T}) = \phi_{{}^t\overline{T}AT}(X). \tag{4.33}$$

证明 设 $A=(a_{ij})$, $\overline{a}_{ij}=a_{ji}$, $X=(x_{ij})$, $\overline{x}_{ij}=x_{ji}$, $T=(t_{ij})$. 再令 $TX\,{}^t\overline{T}=(x_{ij}^*)$, ${}^t\overline{T}AT=(a_{ij}^*)$. 那么 $x_{ij}^*=\sum_{k=1}^n\sum_{l=1}^n t_{ik}x_{kl}\overline{t}_{jl}$, $a_{ij}^*=\sum_{k=1}^n\sum_{l=1}^n \overline{t}_{ki}a_{kl}t_{lj}$. 注意到 A, X 是 Hermite 矩阵, 易见有

$$\sum_{i=1}^n\sum_{j=1}^n a_{ij}x_{ij}^*=\sum_{i=1}^n\sum_{j=1}^n a_{ij}^*x_{ij}.$$

于是 (4.33) 成立. □

令 $\mathbb{C}_i$ 表示等价类 C_i 在 $\mathcal{H}(n,\,q^2)$ 的群代数 $\mathbb{C}\mathcal{H}(n,q^2)$ 中的形式和, $\mathfrak{S}$ 为由 $\mathbb{C}_0, \mathbb{C}_1, \cdots, \mathbb{C}_n$ 生成的 S 环. 由 $\mathfrak{S}$ 确定的结合方案 $\mathfrak{X}(\mathfrak{S})$ 就是 $\mathrm{Her}(n,\,q^2)$. 令

$$\phi_A(\mathbb{C}_i)=\sum_{X\in C_i}\phi_A(X),\, i=0,\,1,\,\cdots,\,n, \tag{4.34}$$

那么 $\phi_A(\mathbb{C}_i)$ 是 $\mathrm{Her}(n,\,q^2)$ 的邻接矩阵 A_i 的特征值, 属于特征向量 ϕ_A. 由命题 4.12 知, 对于 $A,B\in\mathcal{H}(n,\,q^2)$. 如果

$$\phi_A(\mathbb{C}_i)=\phi_B(\mathbb{C}_i),\, i=0,\,1,\,\cdots,\,n,$$

那么 A 和 B 在同一个等价类中. 定理 1.14 中在 $\mathcal{H}(n,\,q^2)^*$ 上确定的等价类 Y_j 恰为

$$Y_j=\{\phi_A|A\in C_j\},\, j=0,\,1,\,\cdots,\,n.$$

相应地得到 $\mathcal{H}(n,\,q^2)^*$ 上的一个 S 环 $\mathfrak{S}^*$, 而由 $\mathfrak{S}^*$ 确定的结合方案 $\mathfrak{X}(\mathfrak{S}^*)$ 和 $\mathrm{Her}(n,\,q^2)$ 是形式对偶的.

映射 $A\mapsto\phi_A$ 是 $\mathcal{H}(n,\,q^2)$ 到 $\mathcal{H}(n,\,q^2)^*$ 的一个同构对应, 它诱导出结合方案 $\mathrm{Her}(n,\,q^2)$ 和 $\mathfrak{X}(\mathfrak{S}^*)$ 的一个同构. 因此我们得到

定理 4.13 Hermite 矩阵的结合方案 $\mathrm{Her}(n,\,q^2)$ 是自对偶的.

实际上, 由 (4.32) 和 (4.33) 及定理 1.16 可知, 结合方案 $\mathrm{Her}(n,\,q^2)$ 的第一特征值矩阵 $P=(p_i(j))$ 的 (j,i) 位置元素为

$$p_i(j)=\phi_A(\mathbb{C}_i)=\sum_{X\in\mathbb{C}_i}\phi_A(X),\, A\in C_j,$$

由定义 (4.32) 可知 $\phi_A(X)=\phi_X(A)$. 于是通过计算 $\sum_{A\in C_j}\sum_{X\in C_i}\phi_A(X)$ 可得

$$k_jp_i(j)=k_ip_j(i).$$

由此即可导出

$$P^2=|\mathcal{H}(n,q^2)|I.$$

由定理 4.5 和定理 4.13, 立得

定理 4.14 Hermite 矩阵的结合方案 $\mathrm{Her}(n,\,q^2)$ 是 P 和 Q 多项式的.

§4.6 Hermite 矩阵结合方案的自同构

关于 Hermite 矩阵结合方案 Her(n, q^2) 的自同构, 我们有下面的

定理 4.15 设 $n \geqslant 2$. $\mathbb{F}_{q^2}$ 上 n 阶 Hermite 矩阵结合方案 Her(n, q^2) 的自同构具有如下形状:

$$X \longmapsto PX^{\sigma}\,{}^t\overline{P} + H_0, \quad \forall X \in \mathcal{H}(n, q^2), \tag{4.35}$$

这里 $P \in GL_n(\mathbb{F}_{q^2})$, $H_0 \in \mathcal{H}(n, q^2)$, σ 是 $\mathbb{F}_{q^2}$ 的一个自同构.

证明 设 $q = p^t$, p 是素数. 由定理 4.7, 结合方案 Her(n, q^2) 的价 $k_i = H_i(n, q^2)$ 所含素数 p 的幂为 $p^{\frac{1}{2}i(i-1)t}$, $i = 1, \cdots, n$, 它们皆不同, 因而 $k_1, k_2, \cdots, k_n$ 两两不等. 于是由推论 1.28(i), Her(n, q^2) 的每个自同构都是内自同构.

再由定理 4.4. Her(n, q^2) 的关系图 $\Gamma^{(1)}$ 是距离正则的, 因而 Aut(Her(n, q^2)) = Aut$\Gamma^{(1)}$.

最后, 由 Hermite 矩阵几何基本定理 [16] 知, 图 $\Gamma^{(1)}$ 的自同构具有形状 (4.35). 于是定理得证. □

第五章　对称矩阵的结合方案 (特征数 $\neq 2$)

§5.1　对称矩阵的合同标准形

设 $\mathbb{F}_q$ 是 q 个元素的有限域, 这里 q 是一个奇素数的幂. 熟知, $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ 对于 $\mathbb{F}_q$ 的乘法作成一个循环群, 而且它的平方元的集合作成 $\mathbb{F}_q^*$ 的一个子群, 记作 $\mathbb{F}_q^{*2}$. 显然,$\mathbb{F}_q^* : \mathbb{F}_q^{*2} = 2$. 我们再把 $\mathbb{F}_q^*$ 的非平方元的集合记作 $z\mathbb{F}_q^{*2}$, 其中 z 是 $\mathbb{F}_q^*$ 中取定的一个非平方元, 那么 $|\mathbb{F}_q^{*2}| = |z\mathbb{F}_q^{*2}| = \frac{1}{2}|\mathbb{F}_q^*| = \frac{1}{2}(q-1)$. 设 g 是群 $\mathbb{F}_q^*$ 的一个生成元, 由群 $\mathbb{F}_q^*$ 的阶是 $q-1$, 可知 $g^{q-1}=1$, 所以 $g^{\frac{1}{2}(q-1)} = -1$. 因此 $-1 \in \mathbb{F}_q^{*2}$ 当且仅当 $q \equiv 1 \pmod 4$.

本章中恒设 q 为奇素数的幂.

引理 5.1　$\mathbb{F}_q^*$ 中的每个非平方元总可表成两个平方元的和.

证明　显然, 只需证明至少有一个非平方元可表成两个平方元之和即可. 假设任二平方元之和仍为平方元, 设 $\mathbb{F}_q^{*2}$ 中的元素为 $a_1, \cdots, a_m$, 这里 $m = \frac{1}{2}(q-1)$. 任取 a_i, 考虑 $a_i + a_1, \cdots, a_i + a_m$, 如果它们皆不为 0, 那么应有某个 a_k 使 $a_i + a_k = a_i$, 因而 $a_k = 0$, 矛盾, 于是有某个 $a_j = -a_i$. 这样,$\mathbb{F}_q^{*2} \cup \{0\}$ 为 $\mathbb{F}_q$ 的一个加法子群. 任 $|\mathbb{F}_q^{*2} \cup \{0\}| = \frac{1}{2}(q+1)$ 不是 $|\mathbb{F}_q| = q$ 因子, 矛盾. □

设 $n \geqslant 1$,$\mathbb{F}_q$ 上 $n \times n$ 矩阵 $A = (a_{ij})$ 叫做对称的, 如果 $a_{ij} = a_{ji}$. 两个 $n \times n$ 对称矩阵 A 和 B 说是合同的, 记作 $A \sim B$, 如果存在 $T \in GL_n(\mathbb{F}_q)$ 使得 $TA{}^tT = B$. 显然, 合同是一个等价关系. 在这一节中我们讨论 $\mathbb{F}_q$ 上 n 阶对称矩阵的合同标准形.

引理 5.2　设 z 是 $\mathbb{F}_q$ 的一个非平方元. 那么 $\mathbb{F}_q$ 上 2×2 对角矩阵

$$[1, 1] \text{ 和 } [z, z]$$

合同.

证明　由引理 5.1, 方程 $1 + x^2 = zw^2$ 在 $\mathbb{F}_q^*$ 中一定有解. 不妨设 (a, b) 是它的一个解. 即 $1 + a^2 = zb^2$, 那么

$$\begin{pmatrix} \frac{1}{zb} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix} {}^t\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} {}^t\begin{pmatrix} \frac{1}{zb} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \frac{a}{b} \\ \frac{a}{b} & z \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 \\ -a & b \end{pmatrix} \begin{pmatrix} 1 & \frac{a}{b} \\ \frac{a}{b} & z \end{pmatrix} {}^t\begin{pmatrix} 1 & 0 \\ -a & b \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

因此 $[1, 1] \sim [z, z]$. □

为了书写简便, 我们用 $[A_1, A_2, \cdots, A_t]$ 表示主对角线上依次是方阵 A_1, $A_2, \cdots, A_t$ 的分块对角矩阵, 用 $I^{(r)}$ 表示 r 阶单位矩阵.

定理 5.3 设 A 是 $\mathbb{F}_q$ 上的 $n \times n$ 对称矩阵, 那么

$$A \sim [I^{(r)}, 0^{(n-r)}], \tag{5.1}$$

或

$$A \sim [I^{(r-1)}, z, 0^{(n-r)}], \tag{5.2}$$

并且形如 (5.1) 和 (5.2) 的两个矩阵不合同.

证明 设 $A \neq 0$, $\operatorname{rank} A = r \geqslant 1$. 从线性代数可知

$$A \sim [a_1, \cdots, a_r, 0 \cdots, 0], a_i \neq 0, i = 1, 2, \cdots, r.$$

通过交换行和相应的列, 不妨设 $a_1, \cdots, a_l$ 是平方元,$a_{l+1}, \cdots, a_r$ 是非平方元. 令 $a_1 = b_1^2, \cdots, a_l = b_l^2$, $a_{l+1} = zb_{l+1}^2, \cdots, a_r = zb_r^2$, $b_{r+1} = \cdots = b_n = 1$. 那么

$$\begin{aligned}&[b_1^{-1}, b_2^{-1}, \cdots, b_n^{-1}][a_1, \cdots, a_r, 0 \cdots, 0]\,{}^t[b_1^{-1}, b_2^{-1}, \cdots, b_n^{-1}]\\ =&[I^{(l)}, zI^{(r-l)}, 0^{(n-r)}].\end{aligned}$$

当 $l = r$ 时, 显然 (5.1) 成立.$r - l$ 是正偶数时, 由引理 5.2 可以得到 (5.1); 当 $r - l$ 是正奇数时, 可由引理 5.2 得到 (5.2).

现在, 假设 $[I^{(r)}, 0^{(n-r)}] \sim [I^{(r-1)}, z, 0^{(n-r)}]$, 于是有非奇异 $n \times n$ 矩阵

$$\begin{pmatrix} P & Q \\ R & S \end{pmatrix} \begin{matrix} r \\ n-r \end{matrix}$$

使得

$$\begin{pmatrix} P & Q \\ R & S \end{pmatrix} \begin{pmatrix} I^{(r)} & \\ & 0^{(n-r)} \end{pmatrix} {}^t\begin{pmatrix} P & Q \\ R & S \end{pmatrix} = \left(\begin{array}{c|c} \begin{matrix} I^{(r-1)} & \\ & z \end{matrix} & \\ \hline & 0^{(n-r)} \end{array}\right).$$

因而有 $P\,{}^tP = [I^{(r-1)}, z]$, 这样就有 $z = (\det P)^2$, 导致矛盾. □

我们把形如 (5.1) 或 (5.2) 的矩阵叫做对称矩阵 A 的合同标准形, 并说 A 是 $(r, 1)$ 型的, 如果 A 的合同标准形如 (5.1); 说 A 是 (r, z) 型的, 如果 A 的合同标准形如 (5.2).

§5.2 对称矩阵结合方案及其本原性

令 $S(n, q)$ 表示 $\mathbb{F}_q$ 上 $n \times n$ 对称矩阵的集合. 因为 $\mathbb{F}_q$ 上的全体 $n \times n$ 矩阵所成的集合 $M_n(\mathbb{F}_q)$ 对于矩阵的加法和纯量乘法做成一个向量空间, 其维数是 n^2. 显

然 $S(n, q)$ 对于矩阵的加法和纯量乘法是封闭的, 所以 $S(n, q)$ 是 $M_n(\mathbb{F}_q)$ 的一个子空间. 注意到

$$\{E_{ii}|1 \leqslant i \leqslant n\} \cup \{E_{ij}+E_{ji}|1 \leqslant i \neq j \leqslant n\}$$

作成 $S(n, q)$ 的一个基, 因而 $\dim S(n, q) = \frac{1}{2}n(n+1)$. 显然 $S(n, q)$ 对于矩阵的加法作成一个加法群, 它的阶为

$$|S(n, q)| = q^{\frac{1}{2}n(n+1)}.$$

$\mathbb{F}_q$ 上的一般线性群 $GL_n(\mathbb{F}_q)$ 如下作用在 $S(n, q)$ 上:

$$\begin{aligned} GL_n(\mathbb{F}_q) \times S(n, q) &\longrightarrow S(n, q) \\ (T, X) &\longmapsto TX\,{}^tT. \end{aligned} \tag{5.3}$$

易见, 每个 $T \in GL_n(\mathbb{F}_q)$ 都给出向量空间 $S(n, q)$ 的一个自同构, 这就给出群在 $S(n, q)$ 上的一个线性表示, 其核是 $\{\pm I^{(n)}\}$.

令 T_0 表示加法群 $S(n, q)$ 的平移群, 并令 G 是由 $GL_n(\mathbb{F}_q)$ 和 T_0 生成的群, 它是 $S(n, q)$ 上的一个置换群, 具体地说,G 的元素 $(T, A)\,(T \in GL_n(\mathbb{F}_q),\ A \in S(n, q))$ 将 $S(n, q)$ 的元素 X 映到

$$X \longmapsto TX\,{}^tT + A. \tag{5.4}$$

群 G 在 $S(n, q)$ 上的作用 (5.4) 是可迁的, 于是由定理 1.3 知,$(G, S(n, q))$ 确定了 $S(n, q)$ 上的一个结合方案, 叫做 $\mathbb{F}_q$ 上 n 阶对称矩阵的结合方案, 记作 $\mathrm{Sym}(n, q)$.

由定理 1.4 可知, 结合方案 $\mathrm{Sym}(n,q)$ 是交换的, 并且其类数等于在 $GL_n(\mathbb{F}_q)$ 的作用 (5.3) 之下 $S(n, q)$ 的非平凡的轨道数.$S(n, q)$ 中的两个矩阵 X 和 Y 在同一个 $GL_n(\mathbb{F}_q)$ 轨道, 当且仅当存在 $T \in GL_n(\mathbb{F}_q)$ 使得 $Y = TX\,{}^tT$. 由定理 5.3 知,n 阶对称矩阵 X 和 Y 在同一个 $GL_n(\mathbb{F}_q)$ 轨道, 当且仅当它们有相同的标准形. 于是结合方案 $\mathrm{Sym}(n, q)$ 的类数是 $2n$.

令

$$C_{(i,\xi)} = \{X \in S(n, q)|X \sim [I^{(i-1)}, \xi, 0^{(n-i)}]\}, \quad 0 \leqslant i \leqslant n, \tag{5.5}$$

对应的结合类

$$R_{(i,\xi)} = \{(X, Y)|Y - X \in C_{(i,\xi)}\}, \quad \xi = 1 \text{或} z.$$

(应注意把 0 记为 $(0,1) = (0,z) = (0,0)$.) 当 $q \equiv 1 \pmod 4$ 时,-1 是 $\mathbb{F}_q$ 的平方元, 所以每个 $R_{(i,\xi)}$ 是对称的, 因而结合方案 $\mathrm{Sym}(n, q)$ 是对称的; 当 $q \equiv 3 \pmod 4$ 时,-1 是非平方元, 所以对于奇数 i, $R_{(i,\xi)}$ 是非对称的, 因而结合方案 $\mathrm{Sym}(n, q)$ 是非对称的. 对于 $\mathrm{Sym}(n, q)$, 我们记 $R_{(i,\xi)}$ 的价为 $k_{(i,\xi)}(n)$. 记交叉数为 $p^{(k,\xi)}_{(i,\eta)(j,\zeta)}$ 或 $p^{(k,\xi)}_{(i,\eta)(j,\zeta)}(n)$.

下面我们讨论对称矩阵结合方案的本原性.

定理 5.4 群 $G = GL_n(\mathbb{F}_q)\cdot T_0$ 作用在 $S(n, q)$ 上是本原的.

证明 从 G 在 $S(n, q)$ 的作用 (5.4) 知,G 的两个元素 $(T_1, A_1), (T_2, A_2)$ 的乘积为

$$(T_1, A_1)(T_2, A_2) = (T_2T_1, T_2A_1{}^tT_2 + A_2).$$

设 $S(n, q)$ 中零矩阵 0 的稳定子 $G_0 = \{(T, 0)|T \in GL_n(\mathbb{F}_q)\}$. 往证 G_0 是 G 的极大子群.

设 N 为 G 的一个子群使得 $G_0 \subseteq N$ 而 $G_0 \neq N$. 那么存在元素 $(P, A) \in N$ 而且 $A \neq 0$. 再由于 $G_0 \subset N$, 所以

$$(P^{-1}, 0)(P, A) = (I, A) \in N. \tag{5.6}$$

令

$$W = \{X \in S(n, q)|(I, X) \in N\}.$$

从 (5.6) 知 $W \neq \{0\}$. 因为

$$(I, X)(I, Y) = (I, X + Y),$$

所以 W 对于加法是封闭的. 进一步, 由 (5.6) 知, $A \in W$. 设 $\operatorname{rank} A = r > 0$, 且 $A \sim [I^{(r-1)}, \xi, 0^{(n-r)}]$, $\xi = 1$ 或 z. 那么从

$$(T^{-1}, 0)(I, A)(T, 0) = (I, TA^tT) \in N$$

推出 $C_{(r,\xi)} \subset W$, 并由上式可知 W 在 $GL_n(\mathbb{F}_q)$ 的作用 (5.3) 下不变. 我们分两种情形进行讨论.

(i) $r = 1$. 这时 $A = [\xi, 0^{(n-1)}]$. 如果 $\xi = 1$, 那么由引理 5.1, 存在 $\beta, \gamma \in \mathbb{F}_q^*$ 使得 $z = \beta^2 + \gamma^2$. 于是

$$\begin{aligned}[z, 0^{(n-1)}] = {} & [\beta, I^{(n-1)}][1, 0^{(n-1)}][\beta, I^{(n-1)}] \\ & +[\gamma, I^{(n-1)}][1, 0^{(n-1)}][\gamma, I^{(n-1)}] \in W.\end{aligned}$$

如果 $\xi = z$, 那么同样有

$$\begin{aligned}[1, 0^{(n-1)}] = {} & \left[\frac{\beta}{z}, I^{(n-1)}\right][z, 0^{(n-1)}]\left[\frac{\beta}{z}, I^{(n-1)}\right] \\ & +\left[\frac{\gamma}{z}, I^{(n-1)}\right][z, I^{(n-1)}]\left[\frac{\gamma}{z}, I^{(n-1)}\right] \in W.\end{aligned}$$

由此可知, 如果 W 含有一个秩为 1 的对称矩阵, 则 W 含有全体秩为 1 的对称矩阵. 再由 W 在 $GL_n(\mathbb{F}_q)$ 作用 (5.3) 下的不变性及对加法封闭, 如果取 $A = [1, 0^{(n-1)}]$, 那么

$$A + \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, I^{(n-2)}\right] A \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, I^{(n-2)}\right] = [I^{(2)}, 0^{(n-2)}] \in W.$$

如果再取 $B = [z, 0^{(n-1)}]$, 那么

$$A + \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, I^{(n-2)}\right] B \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, I^{(n-2)}\right] = [1, z, 0^{(n-2)}] \in W.$$

因而 W 包含全体秩为 2 的对称矩阵. 类似可知, W 含有任意秩的对称矩阵. 于是 $W = S(n, q)$.

(ii) $r \geqslant 2$. 如果 $-1 \in \mathbb{F}_q^{*2}$, 那么 $q \equiv 1(\bmod 4)$. 设 $-1 = \alpha^2$. 那么

$$[\alpha, \cdots, \alpha, 1, \cdots, 1]A[\alpha, \cdots, \alpha, 1, \cdots, 1] + A = [0, \cdots, 0, 2\xi, 0, \cdots, 0] \in W.$$

因为 $2\xi \neq 0$, 所以 W 含有秩为 1 的对称矩阵, 由 (i) 有 $W = S(n, q)$.

如果 $-1 \in z\mathbb{F}_q^{*2}$, 那么 $q \equiv 3\,(\bmod 4)$. 由引理 5.1, 可设 $-1 = \beta^2 + \gamma^2$. 再取 $\alpha \neq 0$, 那么

$$\begin{aligned} &[\beta, \cdots, \beta, \alpha, \cdots, \alpha]A[\beta, \cdots, \beta, \alpha, \cdots, \alpha] \\ &+[\gamma, \cdots, \gamma, 1, \cdots, 1]A[\gamma, \cdots, \gamma, 1, \cdots, 1] + A \\ =&[0, \cdots, 0, (2+\alpha^2)\xi, 0, \cdots, 0]. \end{aligned}$$

如果 $q \geqslant 7$, 那么存在 $\alpha \in \mathbb{F}_q^{*2}$ 使 $2 + \alpha^2 \neq 0$. 于是 W 含有一个秩为 1 的对称矩阵. 由 (i) 又有 $W = S(n, q)$.

因为 $q \equiv 3(\bmod 4)$, 而 $q \leqslant 5$ 时, 必有 $q = 3$. 如果 $\xi = 1$, 就有 $A = [I^{(r-1)}, \xi, 0^{(n-r)}] = [I^{(r)}, 0^{(n-r)}] \in W$. 那么当 r 是偶数时, W 含有合同于 $[I^{(r)}, 0^{(n-r)}]$ 的 $n \times n$ 对称矩阵 $\left[\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, 2I^{(r-2)}, 0^{(n-r)}\right]$, $\left[\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, I^{(r-2)}, 0^{(n-r)}\right]$, 并且有

$$\begin{aligned} &\left[\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, 2I^{(r-2)}, 0^{(n-r)}\right] - \left[\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, I^{(r-2)}, 0^{(n-r)}\right] \\ =&\left[\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, I^{(r-2)}, 0^{(n-r)}\right] \in W, \end{aligned}$$

$$\left[\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, I^{(r-2)}, 0^{(n-r)}\right] - \left[I^{(r)}, 0^{(n-r)}\right] = \left[0, 1, 0^{(n-2)}\right].$$

当 r 是奇数时,W 含有合同于 $[I^{(r)}, 0^{(n-r)}]$ 的 $n \times n$ 对称矩阵 $[1, 2I^{(r-2)}, 0]$, 并且有

$$[1, 2I^{(r-1)}, 0] - [I^{(r)}, 0^{(n-r)}] = [0, I^{(r-1)}, 0^{(n-r)}],$$

$$[I^{(r)}, 0^{(n-r)}] - [0, I^{(r-1)}, 0^{(n-r)}] = [1, 0^{(n-1)}].$$

所以 W 含有一个秩为 1 的对称矩阵. 由 (i) 知 $W = S(n, q)$.

如果 $\xi = z$,那么 $\xi = 2$, 这时 $A = [I^{(r-1)},\ 2,\ 0^{(n-r)}] \in W$, 那么 W 含有合同于 $[I^{(r-1)},\ 2,\ 0^{(n-r)}]$ 的 $\left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ I^{(r-2)},\ 0^{(n-r)}\right]$ 和 $[1,\ 2,\ I^{(r-2)},\ 0^{(n-r)}]$, 所以

$$\begin{aligned}&\left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ I^{(r-2)},\ 0^{(n-r)}\right] + \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ I^{(r-2)},\ 0^{(n-r)}\right] \\ &+[1,\ 2,\ I^{(r-2)},\ 0^{(n-r)}] + [1,\ 2,\ I^{(r-2)},\ 0^{(n-r)}] \\ =&\left[\begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix},\ I^{(r-2)},\ 0^{(n-r)}\right] \in W,\end{aligned}$$

并且 $\left[\begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix},\ I^{(r-2)},\ 0^{(n-r)}\right]$ 合同于 $[I^{(r)},\ 0^{(n-r)}]$. 这又归结到 $\xi = 1$ 的情形. □

由定理 5.4 和定理 1.18, 我们就有

定理 5.5 对称矩阵的结合方案 $\mathrm{Sym}(n,\ q)$ 是本原的, 因而它的结合关系图 $\Gamma^{(i,\xi)}(i \neq 0)$ 是连通的.

§5.3 低阶情形的参数

下面几节主要讨论 n 阶对称矩阵结合方案 $\mathrm{Sym}(n,\ q)$ 的参数计算. 为此, 参数 p^*_{**} 记作 $p^*_{**}(n)$, 即 $p^{(k,\,\xi)}_{(i,\,\eta)\,(j,\,\zeta)}$, 而把 $R_{(i,\,\xi)}(n)$ 的价记作 $k_{(i,\,\xi)}(n)$.

本节讨论 $n = 1, 2$ 的情形. 我们先证明下面的

引理 5.6 设 q 为奇数的幂. 令

$$D_{00} = \{a \in \mathbb{F}_q^{*2} | 1 + a \in \mathbb{F}_q^{*2}\}, \quad F(0,\ 0) = |D_{00}|, \tag{5.7}$$

$$D_{01} = \{a \in \mathbb{F}_q^{*2} | 1 + a \in z\mathbb{F}_q^{*2}\}, \quad F(0,\ 1) = |D_{01}|, \tag{5.8}$$

$$D_{10} = \{a \in z\mathbb{F}_q^{*2} | 1 + a \in \mathbb{F}_q^{*2}\}, \quad F(1,\ 0) = |D_{10}|, \tag{5.9}$$

$$D_{11} = \{a \in z\mathbb{F}_q^{*2} | 1 + a \in z\mathbb{F}_q^{*2}\}, \quad F(1,\ 1) = |D_{11}|, \tag{5.10}$$

那么

(i) 当 $q \equiv 1 \pmod 4$ 时,

$$F(0,1) = F(1,0) = F(1,1) = \frac{1}{4}(q-1),\ F(0,0) = \frac{1}{4}(q-5).$$

(ii) 当 $q \equiv 3 \pmod 4$ 时,

$$F(0,0) = F(1,0) = F(1,1) = \frac{1}{4}(q-3),\ F(0,1) = \frac{1}{4}(q+1).$$

证明 (i) 设 $q \equiv 1 \pmod 4$, 那么 $-1 \in \mathbb{F}_q^{*2}$. 注意到 $1 + (-1) \notin \mathbb{F}_q^{*2}$, 所以由 (5.7) 和 (5.8) 知

$$F(0,0)+F(0,1)=\frac{1}{2}(q-1)-1=\frac{1}{2}(q-3). \tag{5.11}$$

因为对于任意 $a\in z\mathbb{F}_q^{*2}$ 均有 $1+a\neq 0$, 所以由 (5.9) 和 (5.10) 知

$$F(1,0)+F(1,1)=\frac{1}{2}(q-1). \tag{5.12}$$

对于 $a\in D_{10}$, 对应地有唯一的 $b\in \mathbb{F}_q^{*2}$ 使得 $1+a=b$. 用 a 除其两边有 $\frac{1}{a}+1=\frac{b}{a}$. 注意到 $\frac{1}{a}$ 和 $\frac{b}{a}$ 均是非平方元, 所以 $\frac{1}{a}\in D_{11}$. 反过来, 如果 $a\in D_{11}$, 那么如同刚才的推导, 可知 $\frac{1}{a}\in D_{10}$. 所以 $F(1,0)=F(1,1)=\frac{1}{4}(q-1)$.

进一步, 对于 $a\in D_{01}$, 对应地有唯一的 $b\in z\mathbb{F}_q^{*2}$ 使得 $1+a=b$, 这样就有 $1+(-b)=-a$. 因为 $-1\in\mathbb{F}_q^{*2}$, 所以 $-b\in D_{10}$. 反之, 如果 $x\in D_{10}$, 就有 $y\in\mathbb{F}_q^{*2}$ 使得 $1+x=y$. 于是 $1+(-y)=-x$, 而 $-y\in D_{01}$. 因而 $F(0,1)=F(1,0)=\frac{1}{4}(q-1)$. 由 (5.11) 即可得 $F(0,0)=\frac{1}{2}(q-3)-\frac{1}{4}(q-1)=\frac{1}{4}(q-5)$.

(ii) 设 $q\equiv 3 \pmod 4$, 那么 $-1\in z\mathbb{F}_q^{*2}$. 这时 $F(0,0)+F(0,1)=\frac{1}{2}(q-1)$, 而 $F(1,0)+F(1,1)=\frac{1}{2}(q-3)$. 类似于 (i) 中的讨论可知 $F(1,0)=F(1,1)$, $F(0,0)=F(1,1)$, 进而可得 (ii) □

$\mathrm{Sym}(1,q)$ 是一个 $d=2$ 的交换结合方案, 当 $q\equiv 1 \pmod 4$ 时是对称的; 当 $q\equiv 3\pmod 4$ 时是非对称的. 注意到 $S(1,q)=\mathbb{F}_q$, $C_{(1,\xi)}=\xi\mathbb{F}_q^{*2}$, $\xi=1,z$, 因而 $\mathrm{Sym}(1,q)$ 的两个价相等, 并且

$$k_{(1,\xi)}(1)=\frac{1}{2}(q-1),\quad \xi=1,z. \tag{5.13}$$

令 $\xi,\eta,\zeta=1$ 或 z, 参数

$$\begin{aligned} p_{(1,\eta)(1,\zeta)}^{(1,\xi)}(1) &= |\{x\in\mathbb{F}_q | x\in\eta\mathbb{F}_q^{*2}, \xi-x\in\zeta\mathbb{F}_q^{*2}\}| \\ &= |\{a\in\mathbb{F}_q^{*2} | 1+(-\xi^{-1}\eta)a\in\xi^{-1}\zeta\mathbb{F}_q^{*2}\}|. \end{aligned}$$

利用引理 5.1, 可以算出它们的值 (简记作 $p(\xi,\eta,\zeta)$), 见表 5.1.

利用表 5.1 和命题 1.1, 我们得到

定理 5.7 按照顺序 R_0, $R_{(1,1)}$, $R_{(1,z)}$, 结合方案 $\mathrm{Sym}(1,q)$ 的交叉矩阵如下: 当 $q\equiv 1\pmod 4$ 时,

$$B_{(1,1)}=\begin{pmatrix} 0 & 1 & 0 \\ \frac{1}{2}(q-1) & \frac{1}{4}(q-5) & \frac{1}{4}(q-1) \\ 0 & \frac{1}{4}(q-1) & \frac{1}{4}(q-1) \end{pmatrix},$$

$$B_{(1,z)}=\begin{pmatrix} 0 & 0 & 1 \\ 0 & \frac{1}{4}(q-1) & \frac{1}{4}(q-1) \\ \frac{1}{2}(q-1) & \frac{1}{4}(q-1) & \frac{1}{4}(q-5) \end{pmatrix}.$$

表 5.1 $p(\xi,\eta,\zeta)$ 的值

ξ	η	ζ	$q\equiv 1\pmod 4$时$p(\xi,\eta,\zeta)$的值	$q\equiv 3\pmod 4$时$p(\xi,\eta,\zeta)$的值
1	1	1	$\frac{1}{4}(q-5)$	$\frac{1}{4}(q-3)$
1	1	z	$\frac{1}{4}(q-1)$	$\frac{1}{4}(q-3)$
1	z	1	$\frac{1}{4}(q-1)$	$\frac{1}{4}(q-3)$
1	z	z	$\frac{1}{4}(q-1)$	$\frac{1}{4}(q+1)$
z	1	1	$\frac{1}{4}(q-1)$	$\frac{1}{4}(q+1)$
z	1	z	$\frac{1}{4}(q-1)$	$\frac{1}{4}(q-3)$
z	z	1	$\frac{1}{4}(q-1)$	$\frac{1}{4}(q-3)$
z	z	z	$\frac{1}{4}(q-5)$	$\frac{1}{4}(q-3)$

这时关系图 $\Gamma^{(1,1)}$ 和 $\Gamma^{(1,z)}$ 都是距离正则的.

当 $q\equiv 3(\mathrm{mod}\,4)$ 时,

$$B_{(1,1)}=\begin{pmatrix}0&1&0\\0&\frac{1}{4}(q-3)&\frac{1}{4}(q+1)\\\frac{1}{2}(q-1)&\frac{1}{4}(q-3)&\frac{1}{4}(q-3)\end{pmatrix},$$

$$B_{(1,z)}=\begin{pmatrix}0&0&1\\\frac{1}{2}(q-1)&\frac{1}{4}(q-3)&\frac{1}{4}(q-3)\\0&\frac{1}{4}(q+1)&\frac{1}{4}(q-3)\end{pmatrix}.$$

Sym(1, q) 的关系图 $\Gamma^{(1,1)}$ 称为 Paley 图. 当 $q\equiv 3(\mathrm{mod}\,4)$ 时又称为 Paley tournament (参看 [2], [3]).

下面设 $n=2$, Sym(2, q) 是一个 $d=4$ 的交换结合方案, 当 $q\equiv 1\pmod 4$ 时, 它是对称的, 它的足标 $(i,\xi)'=(i,\xi)$; 当 $q\equiv 3\pmod 4$ 时, 它不是对称的, 它的足标有

$$(1,1)'=(1,z),(1,z)'=(1,1),\ (2,\xi)'=(2,\xi),$$

这里 $\xi=1$ 或 z.

容易计算下面的参数

(i) $k_{(1,\xi)}(2)=\frac{1}{2}(q^2-1)$, $\xi=1$或z.

(ii) $k_{(2,\xi)}(2) = \begin{cases} \frac{1}{2}(q^2-1)q, & \text{如果 } -\xi \in \mathbb{F}_q^{*2}, \\ \frac{1}{2}(q-1)^2 q, & \text{如果 } -\xi \notin \mathbb{F}_q^{*2}. \end{cases}$

(iii) $p_{(1,\eta)(1,\zeta)}^{(1,\xi)}(2) = p_{(1,\eta)(1,\zeta)}^{(1,\xi)}(1)$.

(iv) $p_{(1,\eta)(2,\zeta)}^{(1,\xi)}(2) = \begin{cases} \frac{1}{2}(q-1)q, & \text{如果 } -\zeta^{-1}\xi\eta \in \mathbb{F}_q^{*2}, \\ 0, & \text{如果 } -\zeta^{-1}\xi\eta \notin \mathbb{F}_q^{*2}. \end{cases}$

(v) $p_{(2,\eta)(2,\zeta)}^{(1,\xi)}(2) = \begin{cases} \frac{1}{4}(q-1)^2 q, & \text{如果 } \eta \neq \zeta, \\ \frac{1}{4}(q^2-1)q, & \text{如果 } \eta = \zeta \text{ 而 } -\eta \in \mathbb{F}_q^{*2}, \\ \frac{1}{4}(q-1)(q-3)q, & \text{如果 } \eta = \zeta \text{ 而 } -\eta \notin \mathbb{F}_q^{*2}. \end{cases}$

这里给出 (v) 的证明, 其余的请读者自证之.

设 $A = \begin{pmatrix} \xi & 0 \\ 0 & 0 \end{pmatrix}$. 那么

$$p_{(2,\eta)(2,\zeta)}^{(1,\xi)}(2) = \left| \left\{ X = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \middle| \det X \in \eta \mathbb{F}_q^{*2}, \det(A - X) \in \zeta \, \mathbb{F}_q^{*2} \right\} \right|.$$

矩阵 X 的元素 a, b, c 满足下面方程组

$$\begin{cases} ac - b^2 = \eta x^2 & (x^2 \neq 0), \\ (a-\xi)c - b^2 = \zeta y^2 & (y^2 \neq 0). \end{cases}$$

由此可导出 $\xi c = \eta x^2 - \zeta y^2$. 如果 $\eta \neq \zeta$, 那么 $c \neq 0$. 这时任取 $x^2, y^2 \in \mathbb{F}_q^{*2}$ 及 $b \in \mathbb{F}_q$, 令 $c = \xi^{-1}(\eta x^2 - \zeta y^2), a = c^{-1}(b^2 + \eta x^2)$, 这样的选取数为 $\frac{1}{4}(q-1)^2 q$.

现在设 $\eta = \zeta$, 于是 $\xi c = \eta(x^2 - y^2)$. 如果 $-\eta \notin \mathbb{F}_q^{*2}$, 那么 $c \neq 0$, 因而 $x^2 \neq y^2$. 选取这样的 x^2 及 y^2, 令 $c = \xi^{-1}\eta(x^2 - y^2)$. 再任取 b, 令 $a = c^{-1}(b^2 + \eta x^2)$, 这样的选取数为 $\frac{1}{4}(q-1)(q-3)q$.

最后设 $\eta = \zeta$ 且 $-\eta \in \mathbb{F}_q^{*2}$. 这时对于 $x^2 = y^2$ 的对子我们有 $c = 0$, 因而 $-b^2 = \eta x^2$. 我们可选取 $b \neq 0$, 而任意选取 a. 这样的选取数为 $(q-1)q$, 连同如上 $c \neq 0$ 时选取数一起得 $\frac{1}{4}(q^2-1)q$. □

关于参数 $p_{(2,\eta)(2,\zeta)}^{(2,\xi)}(2)$ 的计算, 利用命题 1.1(vi), 只需讨论 $\zeta = \eta$ 的情形, 我们有

定理 5.8

(i) 当 $q \equiv 1 \pmod 4$ 时,

$$p_{(2,1)(2,1)}^{(2,1)}(2) = \frac{1}{4}(q-3)^2(q-1) + (q-2)(2q-1),$$

$$p_{(2,z)(2,z)}^{(2,1)}(2) = \frac{1}{4}(q-1)^3,$$

$$p_{(2,1)(2,1)}^{(2,z)}(2) = \frac{1}{4}(q^2-1)(q-1),$$

$$p_{(2,z)(2,z)}^{(2,z)}(2) = \frac{1}{4}(q-3)^2(q+1)+q-2.$$

(ii) 当 $q \equiv 3 \pmod 4$ 时,

$$p_{(2,1)(2,1)}^{(2,1)}(2) = \frac{1}{4}(q-3)^2(q+1)+q-2,$$

$$p_{(2,z)(2,z)}^{(2,1)}(2) = \frac{1}{4}(q^2-1)(q-1),$$

$$p_{(2,1)(2,1)}^{(2,z)}(2) = \frac{1}{4}(q-1)^3,$$

$$p_{(2,z)(2,z)}^{(2,z)}(2) = \frac{1}{4}(q-3)^2(q-1)+(q-2)(2q-1).$$

证明 我们将 (i), (ii) 合在一起给出证明, 就是说, 讨论 $p_{(2,\eta)(2,\eta)}^{(2,\xi)}(2)$ 的计算. 设 $A = \begin{pmatrix} 1 & 0 \\ 0 & \xi \end{pmatrix}$, 并令

$$M_{(2,\eta)(2,\eta)}^{(2,\xi)} = \{X = \begin{pmatrix} a & b \\ b & c \end{pmatrix} | \det X \in \eta \mathbb{F}_q^{*2}, \det (A-X) \in \eta \mathbb{F}_q^{*2}\}.$$

那么 $p_{(2,\eta)(2,\eta)}^{(2,\xi)}(2) = |M_{(2,\eta)(2,\eta)}^{(2,\xi)}|$. 矩阵 $X = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \in M_{(2,\eta)(2,\eta)}^{(2,\xi)}$, 意味着下面的等式成立:

$$ac - b^2 = \eta x^2,\ (a-1)(c-\xi) - b^2 = \eta y^2\ (x^2 \neq 0,\ y^2 \neq 0).$$

由此容易看出 $a\xi$ 和 c 是二次方程

$$\lambda^2 - (\xi + \eta x^2 - \eta y^2)\lambda + \xi(b^2 + \eta x^2) = 0 \tag{5.14}$$

的根, 而此二次方程在 $\mathbb{F}_q$ 中有根的条件是

$$(\xi + \eta x^2 - \eta y^2)^2 - 4\xi(b^2 + \eta x^2) = z^2. \tag{5.15}$$

我们就是要在 $x^2 \neq 0$ 和 $y^2 \neq 0$ 的条件下从 (5.14) 和 (5.15) 求出 a, b, c, 进而计算所要求的矩阵 X 的个数.

令 $D = (\xi + \eta x^2 - \eta y^2)^2 - 4\xi\eta x^2$, 那么 (5.15) 可写作

$$D = 4\xi b^2 + z^2. \tag{5.16}$$

(1) 设 $\xi \neq \eta$. 那么 $\xi\eta$ 不是平方元, 因而对于任意 $x^2 \neq 0$ 和 $y^2 \neq 0$ 均有 $D \neq 0$. 我们考虑满足条件 (5.16) 的对子 (b^2, z^2).

设 D 为平方元. 如果 $\xi=1(\eta=z)$, 那么满足条件 (5.16) 的对子 (b^2, z^2) 有 $(\frac{1}{4}D,0)$, $(0, D)$ 和 t 个使 b^2 和 z^2 均不为 0 的对子. 由引理 5.6, 这里.

$$t=\begin{cases}F(0,0)=\dfrac{1}{4}(q-5), & \text{如果 } q\equiv 1(\text{mod}4),\\ F(1,0)=\dfrac{1}{4}(q-3), & \text{如果 } q\equiv 3(\text{mod}4).\end{cases}$$

对于对子 $(\frac{1}{4}D, 0)$, 由于 $z^2=0$ 可知方程 (5.14) 有重根 $\lambda=\frac{1}{2}(1+zx^2-zy^2)$, 这样可得 2 个满足要求的矩阵 $\begin{pmatrix}\lambda & b\\ b & \lambda\end{pmatrix}$, $\begin{pmatrix}\lambda & -b\\ -b & \lambda\end{pmatrix}$; 对于对子 $(0, D)$, 方程 (5.14) 的根 $\lambda_1\neq\lambda_2$, 可得到 2 个满足要求的矩阵 $\begin{pmatrix}\lambda_1 & 0\\ 0 & \lambda_2\end{pmatrix}$, $\begin{pmatrix}\lambda_2 & 0\\ 0 & \lambda_1\end{pmatrix}$. 对于 $b^2\neq 0$ 和 $z^2\neq 0$ 的对子 (b^2,z^2), 我们可得到 4 个满足要求的矩阵 $\begin{pmatrix}\lambda_1 & b\\ b & \lambda_2\end{pmatrix}$, $\begin{pmatrix}\lambda_2 & b\\ b & \lambda_1\end{pmatrix}$, $\begin{pmatrix}\lambda_1 & -b\\ -b & \lambda_2\end{pmatrix}$ 和 $\begin{pmatrix}\lambda_2 & -b\\ -b & \lambda_1\end{pmatrix}$. 因此, 对于使 D 为非 0 平方元的对子 (x^2, y^2), 我们得到满足要求的矩阵个数分别为 $q-1$(当 $q\equiv 1\,(\text{mod } 4)$) 或 $q+1$(当 $q\equiv 3\,(\text{mod } 4)$). 如果 $\xi=z(\eta=1)$, 那么满足 (5.16) 对子 (b^2, z^2) 有 $(0, D)$ 和 t' 个使 b^2 和 z^2 均不为 0 的对子, 由引理 5.6 知, 这里

$$t'=\begin{cases}F(1,0)=\dfrac{1}{4}(q-1), & \text{如果 } q\equiv 1\,(\text{mod}\,4),\\ F(0,0)=\dfrac{1}{4}(q-3), & \text{如果 } q\equiv 3\,(\text{mod}\,4).\end{cases}$$

如上讨论可得满足要求的矩阵个数分别为 $q+1$(当 $q\equiv 1\,(\text{mod } 4)$) 和 $q-1$(当 $q\equiv 3\,(\text{mod } 4)$).

设 D 为非平方元, 仿上讨论可知, 如果 $\xi=1(\eta=z)$, 可得满足要求的矩阵个数也分别为 $q-1$ (当 $q\equiv 1\,(\text{mod } 4)$) 和 $q+1$(当 $q\equiv 3\,(\text{mod } 4)$). 如果 $\xi=z(\eta=1)$, 可得满足要求的矩阵个数也分别为 $q+1$(当 $q\equiv 1\,(\text{mod } 4)$) 和 $q-1$(当 $q\equiv 3\,(\text{mod } 4)$).

由于 $\xi\neq\eta$, 使 $D\neq 0$ 的对子 $(x^2, y^2)(x^2\neq 0, y^2\neq 0)$ 的个数为 $\frac{1}{4}(q-1)^2$, 从上面的讨论立得本定理中 (i) 和 (ii) 中第 2, 3 的结论.

(2) 设 $\xi=\eta$. 这时,D 可有如下的分解

$$D=\xi^2[(x+1)^2-y^2][(x-1)^2-y^2].$$

如果 $x^2=1$, 那么有且仅有一个 $y^2\neq 0$ 使 $D=0$; 如果 $x^2\neq 1$(注意 $x^2\neq 0$), 那么有且仅有两个 $y^2\neq 0$ 使 $D=0$. 因此, 使 $D=0$ 的对子 (x^2, y^2) 的个数为 $q-2$, 而使 $D\neq 0$ 的对子 (x^2, y^2) 的个数为 $\frac{1}{4}(q-3)^2$.

设 (x^2, y^2) 为使 $D=0$ 的一个对子, 那么满足 (5.16) 的对子 (b^2, z^2) 有 $(0,0)$ 和 s 个使 b^2 和 z^2 均不为 0 的对子, 这里 $s=0$, 如果 $-\xi\notin\mathbb{F}_{q^*}^2$; $s=\frac{1}{2}(q-1)$, 如果 $-\xi\in\mathbb{F}_q^{2*}$; 对于对子 $(0,0)$, 可知方程 (5.14) 有重根 $\lambda=\frac{1}{2}\xi(1+x^2-y^2)$, 我们可得

t 个满足要求的矩阵 $\begin{pmatrix} \xi^{-1}\lambda & 0 \\ 0 & \lambda \end{pmatrix}$. 对于 b^2 和 z^2 均不为 0 的对子我们可得 $4s$ 个满足要求的矩阵. 因此在 $D=0$ 的情形, 我们可得满足要求的矩阵个数为

$$\begin{cases} q-2, & \text{如果 } -\xi \notin \mathbb{F}_q^{*2}, \\ (q-2)(2q-1), & \text{如果 } -\xi \in \mathbb{F}_q^{*2}. \end{cases}$$

对于 $\frac{1}{4}(q-3)^2$ 个使 $D \neq 0$ 的对子 (x^2, y^2), 如同 (1) 中那样讨论, 可得满足要求的矩阵个数分别

$$\begin{cases} \dfrac{1}{4}(q-3)^2(q+1), & \text{如果 } -\xi \notin \mathbb{F}_q^{*2}, \\ \dfrac{1}{4}(q-3)^2(q-1), & \text{如果 } -\xi \in \mathbb{F}_q^{*2}. \end{cases}$$

这样我们就得到本定理中 (i) 和 (ii) 之第 1 和第 4 的结论. □

§5.4 正交几何中的几个计数公式

关于对称矩阵结合方案 Sym(n, q) 的参数计算, 和前面几章一样, 我们将利用 [15] 中关于正交几何中的一些计数公式 (可参看 [15] 的第六章).

$\mathbb{F}_q$ 上 $n \times n$ 非奇异对称矩阵 $A=(a_{ij})(a_{ij}=a_{ji})$ 叫做定号的, 如果任意 n 维行量 $v=(x_1,\cdots,x_n)$ 使 $vA\,{}^tv=0$, 必有 $v=0$. 利用引理 5.1 不难证明,$\mathbb{F}_q$ 上定号矩阵的阶 $n \leqslant 2$.

现在, 我们给出 $\mathbb{F}_q$ 上对称矩阵的另一种合同标准形, 设 $n=2\nu+\delta, \delta=0,1$ 或 2. z 为 $\mathbb{F}_q$ 中一个取定的非平方元. 令

$$S_{2\nu+\delta,\Delta} = \left[\begin{pmatrix} 0 & I^{(\nu)} \\ I^{(\nu)} & 0 \end{pmatrix}, \Delta\right], \tag{5.17}$$

这里

$$\Delta = \begin{cases} \varnothing\,(\text{不出现}), & \text{如果 } \delta=0, \\ 1 \text{ 或 } z, & \text{如果 } \delta=1, \\ [1,\, z], & \text{如果 } \delta=2. \end{cases}$$

Δ 是 $S_{2\nu+\delta,\Delta}$ 的定号部分 (当 $\delta \neq 0$ 时),ν 称为 $S_{2\nu+\delta,\Delta}$ 的指数 (index).

通过计算 $\det S_{2s+\delta,\Delta}$, 由定理 5.3 可得下面的论断:

设 S 是 $\mathbb{F}_q$ 上秩为 r 的一个 $n \times n$ 对称矩阵. 如果 r 是奇数, 记 $r=2s+1$, 那么 S 合同于

$$[S_{2s+1,1},\, 0^{(n-r)}] \text{ 或 } [S_{2s+1,z},\, 0^{(n-r)}], \tag{5.18}$$

并且这两个矩阵不合同.

如果 r 是偶数, 记 $r=2s$, 那么 S 合同于

$$[S_{2s,\varnothing},\ 0^{(n-r)}] \text{或} \ [S_{2(s-1)+2,[1,-z]},0^{(n-r)}], \tag{5.19}$$

并且这两个矩阵不合同.

矩阵 (5.18) 和 (5.19) 称为 L. E. Dickson *标准形*.

设 $n=2\nu+\delta$, $\nu \geqslant 0$, $\delta=0$, 1, 或 2. $\mathbb{F}_q$ 上的一个 $(2\nu+\delta)\times(2\nu+\delta)$ 矩阵 T 叫做一个*关于* $S_{2\nu+\delta,\Delta}$ *的正交矩阵*, 如果 T 满足

$$TS_{2\nu+\delta,\Delta}\,{}^tT=S_{2\nu+\delta,\Delta}. \tag{5.20}$$

易知, 全体 $(2\nu+\delta)\times(2\nu+\delta)$ 正交矩阵对于矩阵的乘法作成 $GL_n(\mathbb{F}_q)$ 的一个子群, 叫做 $\mathbb{F}_q$ 上关于 $S_{2\nu+\delta,\Delta}$ 的 $2\nu+\delta$ *级正交群*, 记作 $O_{2\nu+\delta,\Delta}(\mathbb{F}_q)$. 由 [15] 中定理 6.21, $O_{2\nu+\delta,\Delta}$ 的阶为

$$|O_{2\nu+\delta,\Delta}(\mathbb{F}_q)|=q^{\nu(\nu+\delta-1)}\prod_{i=1}^{\nu}(q^i-1)\prod_{i=0}^{\nu+\delta-1}(q^i+1). \tag{5.21}$$

注意到,$TS_{2\nu+\delta,\Delta}\,{}^tT=S_{2\nu+\delta,\Delta}$ 当且仅当 ${}^tTS^{-1}_{2\nu+\delta,\Delta}T=S^{-1}_{2\nu+\delta,\Delta}$, 并且 $S_{2\nu+\delta,\Delta}$ 和 $S^{-1}_{2\nu+\delta,\Delta}$ 有相同的类型. 又易见 $S^{-1}_{2\nu+\delta,\Delta}=S_{2\nu+\delta,\Delta^{-1}}$, 这里当 $\delta=0$ 时 Δ^{-1} 仍为 $\varnothing$.

令 $\mathbb{F}_q^{(2\nu+\delta)}$ 表示 $\mathbb{F}_q$ 上 $(2\nu+\delta)$ 维行向量空间. 正交群 $O_{2\nu+\delta,\Delta}(\mathbb{F}_q)$ 自然地作用在 $\mathbb{F}_q^{(2\nu+\delta)}$ 上如下:

$$\begin{array}{rcl}\mathbb{F}_q^{(2\nu+\delta)}\times O_{2\nu+\delta,\Delta}(\mathbb{F}_q) & \longrightarrow & \mathbb{F}_q^{(2\nu+\delta)} \\ ((x_1,\cdots,x_{2\nu+\delta}),T) & \longmapsto & (x_1,\cdots,x_{2\nu+\delta})T.\end{array} \tag{5.22}$$

向量空间 $\mathbb{F}_q^{(2\nu+\delta)}$ 连同正交群 $O_{2\nu+\delta,\Delta}(\mathbb{F}_q)$ 在它上面的作用称为*正交空间*. 正交矩阵在 $\mathbb{F}_q^{(2\nu+\delta)}$ 上的作用是线性的, 因而自然地作用在 $\mathbb{F}_q^{(2\nu+\delta)}$ 的子空间的集合上.

设 P 是 $\mathbb{F}_q^{(2\nu+\delta)}$ 的一个 m 维子空间, 仍用 P 作为它的一个矩阵表示. 那么 $PS_{2\nu+\delta,\Delta}\,{}^tP$ 合同于

$$M(m,\,2s+\gamma,\,s,\,\Gamma):=[S_{2s+\gamma,\Gamma},\,0^{(m-2s-\gamma)}],$$

其中 $0\leqslant s\leqslant[(m-\gamma)/2]$, $\gamma=0$, 1, 或 2, 并且

$$\Gamma=\begin{cases}\varnothing, & \text{如果 } \gamma=0,\\ 1\text{或}\,x, & \text{如果 } \gamma=1,\\ [1,-z], & \text{如果 } \gamma=2.\end{cases}$$

我们称上述的 m 维子空间 P 为 $\mathbb{F}_q^{(2\nu+\delta)}$ 上关于 $S_{2\nu+\delta,\Delta}$ 的 $(m,\, 2s+\gamma,\, s,\, \Gamma)$ 型子空间. 如果对称矩阵 $S_{2\nu+\delta,\Delta}$ 和正交空间可从上下文看出时, 就可以把 P 简单说成 $(m,\, 2s+\gamma,\, s,\, \Gamma)$ 型子空间. 我们把 $(m,\, 0,\, 0,\, \varnothing)$ 型子空间说成是 m 维全迷向子空间, 并把 $(2s+\gamma,\, 2s+\gamma,\, s,\, \Gamma)$ 型子空间说成是 $2s+\gamma$ 维非迷向子空间. 正交空间中的向量 v 称为迷向的, 或非迷向的, 如果分别有 $vS_{2\nu+\delta,\Delta}{}^tv=0$ 或 $vS_{2\nu+\delta,\Delta}{}^tv\neq 0$. 显然, 非零向量 v 是迷向的, 或非迷向的, 当且仅当由 v 生成的 1 维子空间 $\langle v\rangle$ 分别是全迷向的, 或非迷向的.

在正交群 $O_{2\nu+\delta,\Delta}(\mathbb{F}_q)$ 的作用下 $\mathbb{F}_q^{(2\nu+\delta)}$ 中类型相同的子空间组成一个轨道. 令 $\mathcal{M}(m,\, 2s+\gamma,\, s,\, \Gamma;\, 2\nu+\delta,\, \Delta)$ 表示 $\mathbb{F}_q^{(2\nu+\delta)}$ 中全体 $(m,\, 2s+\gamma,\, s,\, \Gamma)$ 型子空间组成的轨道, 而 $N(m,\, 2s+\gamma,\, s, \Gamma;\, 2\nu+\delta,\, \Delta)$ 表示 $\mathbb{F}_q^{(2\nu+\delta)}$ 中全体 $(m,\, 2s+\gamma,\, s,\, \Gamma)$ 型子空间的个数. 由 [15] 定理 6.26, 如果 $(m,\, 2s+\gamma,\, s,\, \Gamma)$ 满足

$$2s+\gamma\leqslant m\leqslant\begin{cases}\nu+s+\min\{\delta,\,\gamma\}, & \text{如果}\,\delta\neq\gamma, \text{或}\,\delta=\gamma\,\text{而}\,\Gamma=\Delta,\\ \nu+s, & \text{如果}\,\delta=\gamma\,\text{而}\,\Gamma\neq\Delta,\end{cases}\tag{5.23}$$

那么

$$\begin{aligned}&N(m,\, 2s+\gamma,\, s,\, \Gamma;\, 2\nu+\delta,\, \Delta)\\ =&q^{2s(\nu+s-m)+s(\gamma+\delta)-\gamma(m-2s-\gamma)}\frac{\prod\limits_{i=\nu+s-m+\gamma+1}^{\nu}(q^i-1)(q^{i+\delta-1}+1)}{\prod\limits_{i=1}^{s}(q^i-1)\prod\limits_{i=0}^{s+\gamma-1}(q^i+1)\prod\limits_{i=1}^{m-2s-\gamma}(q^i-1)}\\ &\cdot n_0(m,\, 2s+\gamma,\, s,\, \Gamma;\, 2\nu+\delta,\, \Delta),\end{aligned}\tag{5.24}$$

其中

$$\begin{aligned}&n_0(m,\, 2s,\, s;\, 2\nu+\delta,\, \Delta)=1;\\ &\quad n_0\ (m, 2s+1, s, \Gamma; 2\nu+\delta, \Delta)\\ &\quad=\begin{cases}q^{(\nu-s-1)}(q^{\nu+s-m+1}-1), & \text{如果}\,\delta=0.\\ q^{\nu-s}(q^{\nu+s-m+1}-1), & \text{如果}\,\delta=1\,\text{而}\,\Gamma\neq\Delta,\\ q^{\nu-s}(q^{\nu+s-m+1}+1), & \text{如果}\,\delta=1\,\text{而}\,\Gamma=\Delta,\\ q^{\nu-s}(q^{\nu+s-m+2}+1), & \text{如果}\,\delta=2;\end{cases}\end{aligned}\tag{5.25}$$

$$\begin{aligned}&n_0\ (m,\, 2s+2,\, s,\, \Gamma;\, 2\nu+\delta,\, \Delta)\\ &=\begin{cases}q^{2(\nu-s)-2}(q^{\nu+s-m+1}-1)(q^{\nu+s-m+2}-1), & \text{如果}\,\delta=0,\\ q^{2(\nu-s)-1}(q^{\nu+s-m+2}-1)(q^{\nu+s-m+2}+1), & \text{如果}\,\delta=1,\\ q^{2(\nu-s)}(q^{\nu+s-m+2}+1)(q^{\nu+s-m+3}+1), & \text{如果}\,\delta=2.\end{cases}\end{aligned}$$

在后面的计算中, 要用到关于矩阵的一个计数公式.

设 A 是 $\mathbb{F}_q$ 上的一个 $l\times(2\nu+\delta)$ 矩阵, 如果 $AS_{2\nu+\delta,\Delta}\,{}^tA\sim M(m,\,2s+\gamma,\,s,\,\Gamma)$, 就称 A 是关于 $S_{2\nu+\delta,\Delta}$ 的一个 $(m,\,2s+\gamma,\,s,\,\Gamma)$ 型矩阵, 这里 $(m,\,2s+\gamma,\,s,\,\Gamma)$ 满足 (5.23). 令 $n(l\times(2\nu+\delta),\,m,\,2s+\gamma,\,s,\,\Gamma;\,2\nu+\delta,\,\Delta)$ 表示 $\mathbb{F}_q$ 上关于 $S_{2\nu+\delta,\Delta}$ 的全体 $(m,\,2s+\gamma,\,s,\,\Gamma)$ 型 $l\times(2\nu+\delta)$ 矩阵的个数, 我们有如下的

定理 5.9 设 $l\geqslant m$, $(m,\,2s+\gamma,\,s,\,\Gamma)$ 满足 (5.23), 那么

$$
\begin{aligned}
&n(l\times(2\nu+\delta);\,m,\,2s+\delta,\,s,\,\Gamma;\,2\nu+\delta,\,\Delta)\\
=&q^{\frac{1}{2}m(m-1)+2s(\nu+s-m)+s(\delta+2)-2(m-2s-2)}\\
&\cdot\frac{\prod\limits_{i=l-m+1}^{l}(q^i-1)\prod\limits_{i=\nu+s-m+\gamma+1}^{\nu}(q^i-1)(q^{i+\delta-1}+1)}{\prod\limits_{i=1}^{s}(q^i-1)\prod\limits_{i=0}^{s+\gamma-1}(q^i+1)\prod\limits_{i=1}^{m-2s-\gamma}(q^i-1)}\\
&\cdot n_0(m,2s+\delta,s,\Gamma;2\nu+\delta,\Delta),
\end{aligned}
\tag{5.26}
$$

其中 $n_0(m,\,2s+\gamma,\,s,\,\Gamma;\,2\nu+\delta,\,\Delta)$ 由 (5.25) 给出.

证明 设 P 是 $\mathbb{F}_q^{(2\nu+\delta)}$ 中取定的一个 $(m,\,2s+\gamma,\,s,\,\Gamma)$ 型子空间,N 是生成 P 的 $l\times(2\nu+\delta)$ 矩阵的个数. 因为 P 是 $\mathbb{F}_q^{(2\nu+\delta)}$ 的一个 m 维子空间, 所以通过交换向量的分量, 可设 P 有形如 $(I^{(m)},\,0^{(m,n-m)})$ 的矩阵表示. 对于任意 $T\in GL_l(\mathbb{F}_q)$, $l\times n$ 矩阵

$$
T\begin{pmatrix} I^{(m)} & 0\\ 0 & 0^{(l-m,n-m)}\end{pmatrix}
$$

的行生成 P, 而且生成 P 的任意 $l\times n$ 矩阵可以取为如上形式的 $l\times n$ 矩阵. 令

$$
G_0'=\left\{T\in GL_l(\mathbb{F}_q)|T\begin{pmatrix} I^{(m)} & 0\\ 0 & 0^{(l-m,n-m)}\end{pmatrix}=\begin{pmatrix} I^{(m)} & 0\\ 0 & 0^{(l-m,n-m)}\end{pmatrix}\right\}.
$$

那么

$$
G_0'=\left\{\begin{pmatrix} I^{(m)} & B\\ 0 & D\end{pmatrix}|D\in GL_{l-m}(\mathbb{F}_q),\,B\text{是任意}m\times(l-m)\text{矩阵}\right\}.
$$

于是

$$
\begin{aligned}
N=GL_l(\mathbb{F}_q):G_0'&=\frac{|GL_l(\mathbb{F}_q)|}{|G_0'|}=\frac{|GL_l(\mathbb{F}_q)|}{|GL_{l-m}(\mathbb{F}_q)|q^{m(l-m)}}\\
&=\prod_{i=l-m+1}^{l}(q^{i-1})q^{\frac{1}{2}m(m-1)}.
\end{aligned}
$$

因为 $\mathbb{F}_q^{(2\nu+\delta)}$ 中关于 $S_{2\nu+\delta,\Delta}$ 的 $(m,\,2s+\gamma,\,s,\,\Gamma)$ 型子空间个数是 $N(m,\,2s+\gamma,\,s,\,\Gamma;2\nu+\delta,\Delta)$, 所以

$$
\begin{aligned}
&n_m\ (l\times(2\nu+\delta),\,m,\,2s+\gamma,\,s,\,\Gamma;2\nu+\delta,\Delta)\\
=&\prod_{i=l-m+1}^{l}(q^{i-1})q^{\frac{1}{2}m(m-1)}N(m,\,2s+\gamma,\,s,\,\Gamma,\,\Delta).
\end{aligned}
$$

由 (5.24) 立得 (5.26). □

§5.5 参数的计算

为了利用 5.4 中给出的计数公式来计算 Sym(n, q) 的参数, 我们有时取对称矩阵的 Dickson 标准形作为合同类的代表元. 具体说, 对于 $S(n,q)$ 的合同类 $C_{(i,\xi)}$ $(i>0)$,

当 $i=2s+1$ 时, 取

$$[S_{2s+1,\eta}, 0^{(n-i)}],\ \text{这里}(-1)^s\eta\in\xi\mathbb{F}_q^{*2}.$$

当 $i=2s$ 时, 取

$$\begin{cases}[S_{2s,\varnothing}, 0^{(n-i)}], & \text{如果}(-1)^s\in\xi\mathbb{F}_q^{*2},\\ [S_{2(s-1)+2,[1,-z]}, 0^{(n-i)}], & \text{如果}(-1)^s z\in\xi\mathbb{F}_q^{*2}.\end{cases} \tag{5.27}$$

先计算价 $k_{(i,\xi)}=|C_{(i,\xi)}|$.

取 $C_{(i,\xi)}$ 的代表 $S=[S_{2s+\gamma,\Gamma}, 0^{(n-i)}]$, S 在 $GL_n(\mathbb{F}_q)$ 中的稳定子 G_s 由满足条件 $TS\,{}^tT=S$ 的矩阵 T 组成. 将 T 相应于 S 分块

$$T=\begin{pmatrix}A & B\\ C & D\end{pmatrix}\begin{matrix}i\\ n-i\end{matrix}.$$
$$\qquad\quad\ i \qquad n-i$$

于是有下面的等式

$$AS_{2s+\gamma,\Gamma}{}^tA=S_{2s+\gamma,\Gamma},\ CS_{2s+\gamma,\Gamma}{}^tA=0.$$

由此可知 $A\in O_{2s+\gamma,\Gamma}(\mathbb{F}_q)$. 特别是 A 非奇异, 所以 $C=0$, $D\in GL_{n-i}(\mathbb{F}_q)$. 这样

$$|G_s|=|O_{2s+\gamma,\Gamma}(\mathbb{F}_q)||GL_{n-i}(\mathbb{F}_q)|q^{i(n-i)},$$

$$|C_{(i,\xi)}|=\frac{|GL_n(\mathbb{F}_q)|}{|O_{2s+\gamma,\Gamma}(\mathbb{F}_q)|GL_{n-i}(\mathbb{F}_q)|q^{i(n-i)}}. \tag{5.28}$$

由 (5.21) 和公式 (2.2) 就得到

定理 5.10 设 $1\leqslant i\leqslant n$, $\xi=1$ 或 z. 如果 $i=2\nu+\delta$, $\delta=0,1$, 或 2,

$$\Delta=\begin{cases}\varnothing, & \text{如果 }\delta=0\text{ 或 }2,\\ 1\text{ 或 }2, & \text{如果 }\delta=1.\end{cases}$$

那么 $\mathbb{F}_q$ 上型为 (i,ξ) 的 n 阶对称矩阵可记作 $S(n, 2\nu+\delta, \nu)$[15], 并且型为 (i, ξ) 的矩阵个数 (记作 $k_{(i,\xi)}(n)$)

$$\begin{aligned}k_{(i,\xi)}(n)&=|S(n,\,2\nu+\delta,\,\nu,\,\Delta)|\\ &=q^{\nu(\nu+\delta)+\frac{1}{2}\delta(\delta-1)}\frac{\prod\limits_{i=\nu+1}^{n}(q^i-1)}{\prod\limits_{i=0}^{\nu+\delta-1}(q^i+1)\prod\limits_{i=1}^{n-2\nu-\delta}(q^i-1)}.\end{aligned}$$

现在来推导 $p^{(k,\xi)}_{(i,\eta),(j,\zeta)}(n)$ 的递推公式. 假定 $n \geqslant 2$. 先考虑 $k<n$ 的情形.

取 $S_1 = 0^{(n)}$, 并且对于 $1 \leqslant k < n$, $\xi = 1$ 或 z. 再取

$$S_2 = [S_{2\nu+\delta,\,\Delta},\, 0^{(n-2\nu-\delta)}]$$

使得 $S_2 \sim [I^{k-1}, \xi, 0^{(n-k)}]$. 令

$$\mathcal{M}^{(k,\xi)}_{(i,\eta),(j,\zeta)} = \{S \in S(n,\, q) | S \sim [I^{(i-1)}, \eta, 0^{(n-i)}], S_2 - S \sim [I^{(j-1)}, \zeta, 0^{(n-j)}]\}.$$

那么

$$p^{(k,\xi)}_{(i,\eta),(j,\zeta)}(n) = |\mathcal{M}^{(k,\xi)}_{(i,\eta),(j,\zeta)}|.$$

令 G_0 是 $[S_{2\nu+\delta,\Delta}, 0^{(n-2\nu-\delta)}]$ 在 $GL_n(\mathbb{F}_q)$ 中的稳定子, 那么 G_0 把 $\mathcal{M}^{(k,\xi)}_{(i,\eta),(j,\zeta)}$ 变成其自已, 并且 G_0 由形如

$$\begin{pmatrix} R & Q \\ 0 & T \end{pmatrix} \begin{matrix} k \\ n-k \end{matrix}$$
$$\begin{matrix} k \quad & n-k \end{matrix}$$

的矩阵组成, 其中 $R \in O_{2\nu+\delta,\Delta}(\mathbb{F}_q)$, $T \in GL_{n-k}(\mathbb{F}_q)$, $Q \in M_{k(n-k)}$. 设 $S \in \mathcal{M}^{(k,\xi)}_{(i,\eta),(j,\zeta)}$, 并把 S 写成如下的分块矩阵

$$S = \begin{pmatrix} U & V \\ {}^tV & W \end{pmatrix} \begin{matrix} k \\ n-k \end{matrix}.$$
$$\begin{matrix} k \quad & n-k \end{matrix}$$

容易验证 G_0 不变块 W 的合同标形. 令

$$\mathcal{M}(t,\rho) = \left\{ \begin{pmatrix} U & V \\ {}^tV & W \end{pmatrix} \in \mathcal{M}^{(k,\xi)}_{(i,\eta),(j,\zeta)} | W \sim [I^{(t-1)},\, \rho,\, 0^{(n-t)}] \right\},$$

其中 $0 \leqslant t \leqslant n-k$, $\rho = 1$ 或 z. 那么

$$\mathcal{M}^{(k,\xi)}_{(i,\eta),(j,\zeta)} = \bigcup_{0 \leqslant t \leqslant n-k,\, \rho=1\text{或}\, z} \mathcal{M}(t,\, \rho).$$

因而

$$p^{(k,\xi)}_{(i,\eta),(j,\zeta)}(n) = \sum_{0 \leqslant t \leqslant n-k,\, \rho=1\text{或}\, z} |\mathcal{M}(t,\, \rho)|. \tag{5.29}$$

为了简单起见, 记 $M_{(t,\,\rho)} = [I^{(t-1)},\, \rho,\, 0^{(n-t)}]$, 并且令

$$\mathcal{M}_1 = \left\{ \begin{pmatrix} U & V_1 & V_2 \\ {}^tV_1 & M_{(t,\rho)} & 0 \\ {}^tV_2 & 0 & 0 \end{pmatrix} \in \mathcal{M}_{(t,\rho)} \right\},$$

那么

$$|\mathcal{M}_{(t,\rho)}| = k_{(t,\rho)}(n-k)|\mathcal{M}_1|. \tag{5.30}$$

对于

$$\begin{pmatrix} U & V_1 & V_2 \\ {}^tV_1 & M_{(t,\rho)} & 0 \\ {}^tV_2 & 0 & 0 \end{pmatrix} \in \mathcal{M}_1,$$

我们取

$$\left[\begin{pmatrix} I & -V_1M_{(t,\rho)}^{-1} \\ & I \end{pmatrix}, I\right] \in G_0,$$

那么

$$\begin{pmatrix} I & -V_1M_{(t,\rho)}^{-1} & \\ & I & \\ & & I \end{pmatrix} \begin{pmatrix} U & V_1 & V_2 \\ {}^tV_1 & M_{(t,\rho)} & 0 \\ {}^tV_2 & 0 & 0 \end{pmatrix} {}^t\begin{pmatrix} I & -V_1M_{(t,\rho)}^{-1} & \\ & I & \\ & & I \end{pmatrix}$$

$$= \begin{pmatrix} U^* & 0 & V_2 \\ 0 & M_{(t,\rho)} & 0 \\ {}^tV_2 & 0 & 0 \end{pmatrix} \in \mathcal{M}_1.$$

设 $\mathcal{M}_2$ 是 $\mathcal{M}_1$ 中形如

$$\begin{array}{c} \begin{pmatrix} U & 0 & V \\ 0 & M_{(t,\rho)} & 0 \\ {}^tV & 0 & 0 \end{pmatrix} \begin{array}{c} k \\ t \\ n-k-t \end{array} \\ \begin{array}{ccc} k & t & n-k-t \end{array} \end{array} \tag{5.31}$$

的矩阵, 那么

$$|\mathcal{M}_1| = q^{kt}|\mathcal{M}_2|. \tag{5.32}$$

注意 (5.31) 中的块 ${}^tV$ 是 $(n-k-t)\times k$ 矩阵. $k = 2\nu+\delta$, $\nu \geqslant 0$, $\delta = 0, 1$, 或 2. 假定 $\operatorname{rank}{}^tV = m$ 并且 ${}^tVS_{2\nu+\delta,\Delta}^{-1}V \sim [S_{2s+\gamma,\Gamma}, 0^{(n-k-t)}]$, 那么 ${}^tV$ 是关于 $S_{2\nu+\delta,\Delta}^{-1}$ 的 $((n-k-t)\times(2\nu+\delta), m, 2s+\gamma, s, \Gamma)$ 型矩阵. 由定理 5.9, 关于 $S_{2\nu+\delta,\Delta}^{-1}$ 的 $((n-k-t)\times(2\nu+\delta), m, 2s+\gamma, s, \Gamma)$ 型矩阵存在当且仅当

$$0 \leqslant m \leqslant n-k-t$$

和 (5.23) 成立. 设 $\mathcal{M}(n-k-t, m, 2s+\gamma, s, \Gamma; 2\nu+\delta, \Delta^{-1})$ 是 $\mathcal{M}_2$ 中形如 (5.31) 的矩阵, 其中 ${}^tV$ 是 $((n-k-t)\times(2\nu+\delta), m, 2s+\gamma, s, \Gamma)$ 型矩阵, 那么

$$|\mathcal{M}_2| = \sum_{m,s,\gamma,\Gamma} |\mathcal{M}(n-k-t, m, 2s+\gamma, s, \Gamma; 2\nu+\delta, \Delta^{-1})|, \tag{5.33}$$

其中 m, s, γ, Γ 满足 (5.23).

我们引进 G_0 的子群 G_1 如下：

$$G_1 = \left\{ \left[R,\, I^{(t)},\, W \right] \Big|\, R \in O_{2\nu+\delta,\Delta}(\mathbb{F}_q), W \in GL_{n-k-t}(\mathbb{F}_q) \right\}.$$

易知 G_1 不改变 ${}^tV$ 关于 $S_{2\nu+\delta,\Delta}^{-1}$ 的类型. 令

$$ {}^tV_0 = \begin{pmatrix} I & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & A & 0 & 0 & B & C \end{pmatrix} \begin{matrix} s \\ s \\ m-2s-\gamma \\ n-k-t-m \\ \gamma \end{matrix} . \tag{5.34}$$
$$\begin{matrix} s & m-2s-\gamma & \nu-m+s+\gamma & s & m-2s-\gamma & \nu-m+s+\gamma & \delta \end{matrix}$$

那么

$${}^tV_0 S_{2\nu+\delta,\Delta}^{-1} V_0 = [S_{2s},\, 0^{(m-2s-\delta)},\, 0^{(m-k-t-m)},\, \Gamma],$$

其中 Γ 是 $\gamma\times\gamma$ 矩阵, 并且 $\Gamma = A\,{}^tB + B\,{}^tA + C\Delta^{-1}\,{}^tC$. 下面的表 5.2 表示对于给定的 δ, Δ 和 γ, Γ, 我们可以选定 A, B, C, 使得 $A\,{}^tB + B\,{}^tA + C\Delta^{-1}\,{}^tC = \Gamma$.

表 5.2　对应于给定的 δ, Δ, γ, Γ 所应选取的 A, B, C

$\delta\gamma$　Δ^{-1}	Γ	A	B	C
0	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
01	1或 z	$\underset{\nu-m+s}{(0}\quad\underset{1}{1)}$	$\underset{\nu-m+s}{(0}\quad\underset{1}{\Gamma/2)}$	$\varnothing$
2	$[1,-z]$	$\underset{\nu-m+s}{(0}\quad\underset{2}{I^{(2)})}$	$\underset{\nu-m+s}{(0}\quad\underset{2}{\Gamma/2)}$	$\varnothing$
0	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
11　1或 z^{-1}	1或 z^{-1}	0	0	1
	z^{-1}或 1	$\underset{\nu-m+s}{(0}\quad\underset{1}{1)}$	$\underset{\nu-m+s}{(0}\quad\underset{1}{\Gamma/2)}$	0
2	$[-\Delta^{-1}z, \Delta^{-1}]$	$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ $\underset{\nu-m+s\quad 1}{}$	$\begin{pmatrix} 0 & -(\Delta^{-1}z)/2 \\ 0 & 0 \end{pmatrix}$ $\underset{\nu-m+s\quad 1}{}$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$
0	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
21 $[1,(-z)^{-1}]$	1	0	0	$(1\ \ 0)$
	z	0	0	$(\mu_1\ \mu_2)$ μ_1, μ_2满足 $\mu_1^2+(-z)^{-1}\mu_2^2=z$
2	$[1,-z]$	0	0	$[1,\ -z]$

设 $\mathcal{M}_3$ 是 $\mathcal{M}(n-k-t,\, m,\, 2s+\gamma,\, s,\, \Gamma;\, 2\nu+\delta,\, \Delta^{-1})$ 中形如

$$\begin{pmatrix} U & 0 & V_0 \\ 0 & M_{(t,\rho)} & 0 \\ {}^tV_0 & 0 & 0 \end{pmatrix} \tag{5.35}$$

的矩阵的集合, 其中 ${}^tV_0$ 由 (5.34) 给出, ${}^tV_0$ 中的 A, B, C 按照表 5.2 来选取. 那么

$$\begin{aligned} &|\mathcal{M}(m-k-t,\, m,\, 2s+\gamma,\, s,\, \Gamma;\, 2\nu+\delta,\, \Delta^{-1})| \\ =&n((n-k-t)\times(2\nu+\delta),\, m,\, 2s+\gamma,\, s,\, \Gamma;\, 2\nu+\delta,\, \Delta^{-1})|\mathcal{M}_3|, \end{aligned} \tag{5.36}$$

其中 $n((n-k-t\times(2\nu+\delta),\, m,\, 2s+\gamma,\, s,\, \Gamma;\, 2\nu+\delta,\, \Delta^{-1})$ 由 (5.26) 给出, 并约定在 $n-k-t=0$ 时, $n((n-k-t)\times(2\nu+\delta),\, m,\, 2s+\gamma,\, s,\, \Gamma;\, 2\nu+\delta,\, \Delta^{-1})=1$.

下面来计算 $|\mathcal{M}_3|$. 我们按照 δ, Δ^{-1}, γ, Γ 的不同取值分别进行讨论, 取 $\gamma=\delta=1$ 和 $\Gamma\neq\Delta^{-1}$ 的情形作为例子. 这时 ${}^tV_0$ 具有如下形式:

$$\begin{array}{c} \begin{pmatrix} I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & \Gamma/2 & 0 \end{pmatrix} \begin{matrix} s \\ s \\ m-2s-\gamma \\ n-k-t-m \\ \gamma \end{matrix} \\ \begin{matrix} s & m-2s-\gamma & \nu-m+s & \gamma & s & m-2s-\gamma & \nu-m+s & \gamma & \delta \end{matrix} \end{array}$$

设 $\mathcal{M}_4$ 是 $\mathcal{M}_3$ 中形如

$$\begin{array}{c} \begin{pmatrix} U & 0 & V_0 \\ 0 & M_{(t,\rho)} & 0 \\ {}^tV_0 & 0 & 0 \end{pmatrix} \begin{matrix} k \\ t \\ n-k-t \end{matrix} \\ \begin{matrix} k & t & n-k-t \end{matrix} \end{array} \tag{5.37}$$

的矩阵, 其中 U 具有如下形式:

$$\begin{array}{c} \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & U_{22} & U_{23} & 0 & 0 & 0 & U_{27} & U_{28} & U_{29} \\ 0 & {}^tU_{23} & U_{33} & 0 & 0 & 0 & U_{37} & U_{38} & U_{39} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & {}^tU_{27} & {}^tU_{37} & 0 & 0 & 0 & U_{77} & U_{78} & U_{79} \\ 0 & {}^tU_{28} & {}^tU_{38} & 0 & 0 & 0 & {}^tU_{78} & U_{88} & U_{89} \\ 0 & {}^tU_{29} & {}^tU_{39} & 0 & 0 & 0 & {}^tU_{79} & {}^tU_{89} & U_{99} \end{pmatrix} \begin{matrix} s \\ m-2s-\gamma \\ \nu-m+s \\ \gamma \\ s \\ m-2s-\gamma \\ \nu-m+s \\ \gamma \\ \delta \end{matrix} \\ \begin{matrix} s & m-2s-\gamma & \nu-m+s & \gamma & s & m-2s-\gamma & \nu-m+s & \gamma & \delta \end{matrix} \end{array} \tag{5.38}$$

那么

$$|\mathcal{M}_3| = q^{\frac{1}{2}(2k+1-m)m}|\mathcal{M}_4|. \tag{5.39}$$

此外, 如果在 $\mathcal{M}_3$ 中形如 (5.35) 的矩阵合同于 $\mathcal{M}_4$ 中形如 (5.37) 的矩阵, 其中 U 由 (5.38) 给出, 那么 $S_2 - S = [S_{2\nu+\delta,\Delta}0^{(n-2\nu-\delta)}] - S$ 合同于形如 (5.37) 的矩阵, 其中 U 具有如下形式:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -U_{22} & -U_{23} & 0 & 0 & 0 & -U_{27} & -U_{28} & -U_{29} \\ 0 & -{}^tU_{23} & -U_{33} & 0 & 0 & 0 & I-U_{37} & -U_{38} & -U_{39} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -{}^tU_{27} & I-{}^tU_{37} & 0 & 0 & 0 & -U_{77} & -U_{78} & -U_{79} \\ 0 & -{}^tU_{28} & -{}^tU_{38} & 0 & 0 & 0 & -{}^tU_{78} & -U_{88}-\Gamma & -U_{89} \\ 0 & -{}^tU_{29} & -{}^tU_{39} & 0 & 0 & 0 & -{}^tU_{79} & -{}^tU_{89} & \Delta-U_{99} \end{pmatrix} \begin{matrix} s \\ m-2s-\gamma \\ \nu-m+s \\ \gamma \\ s \\ m-2s-\gamma \\ \nu-m+s \\ \gamma \\ \delta \end{matrix}.$$
$$\begin{matrix} s & m-2s-\gamma & \nu-m+s & \gamma & s & m-2s-\gamma & \nu-m+s & \gamma & \delta \end{matrix}$$

令

$$\widetilde{U} = \begin{pmatrix} U_{22} & U_{23} & U_{27} & U_{28} & U_{29} \\ {}^tU_{23} & U_{33} & U_{37} & U_{38} & U_{39} \\ {}^tU_{27} & {}^tU_{37} & U_{77} & U_{78} & U_{79} \\ {}^tU_{28} & {}^tU_{38} & {}^tU_{78} & {}^tU_{88} & U_{89} \\ {}^tU_{29} & {}^tU_{39} & {}^tU_{79} & {}^tU_{89} & U_{99} \end{pmatrix},$$

$$\widetilde{U}_1 = 0^{(k-m)}, \quad \widetilde{U}_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I & 0 & 0 \\ 0 & I & 0 & 0 & 0 \\ 0 & 0 & 0 & -\Gamma & 0 \\ 0 & 0 & 0 & 0 & \Delta \end{pmatrix} \begin{matrix} m-2s-\gamma \\ \nu-m+s \\ \nu-m+s \\ \gamma \\ \delta \end{matrix}.$$
$$\begin{matrix} m-2s-\gamma & \nu-m+s & \nu-m+s & \gamma & \delta \end{matrix}$$

从 $S \sim [I^{(i-1)}, \eta, 0^{(n-i)}]$ 得到 $\widetilde{U} \sim [I^{(i-t-2m-1)}, \eta', 0^{(k+m-i+t)}]$, 其中 $\eta' = 1$ 或 z 分别由 $\eta/(-1)^m\rho \in \mathbb{F}_q^{*2}$ 或 $\eta/(-1)^m\rho \in z\mathbb{F}_q^{*2}$ 来取定. 再从 $S_2 - S \sim [I^{(j-1)}, \zeta, 0^{(n-i)}]$ 得到 $\widetilde{U_2} - \widetilde{U} \sim [[I^{(j-t-2m-1)}, \zeta', 0^{(k+m-j+t)}], \zeta' = 1$ 或 z 分别由 $\zeta/(-1)^{m+t}\rho \in \mathbb{F}_q^{*2}$ 或 $\zeta/(-1)^{m+t}\rho \in z\mathbb{F}_q^{*2}$ 来取定. 因而 $\widetilde{U_2} - \widetilde{U_1} \sim [I^{(k-2m+2s+\gamma-1)}, \xi', 0^{(m-2s-\gamma)}]$, $\xi' = 1$ 或 z 分别由 $(-1)^{\nu-m+s}\det(-\Gamma)\det\Delta \in \mathbb{F}_q^{*2}$ 或 $(-1)^{\nu-m+s}\det(-\Gamma)\det\Delta \in z\mathbb{F}_q^{*2}$ 来取定. 于是

$$|\mathcal{M}_4| = p^{(k-2m+2s+\gamma,\xi')}_{(i-t-2m,\eta')(j-t-2m,\zeta')}(k-m). \tag{5.40}$$

从 (5.29), (5.30), (5.32), (5.33), (5.36), (5.39) 和 (5.40) 就得到如下的

定理 5.11 设 $1 \leqslant i, j \leqslant n$, $1 \leqslant k < n$, 而 $\xi, \eta, \zeta = 1$ 或 z. 对于给定的 k, ξ, 令 $k = 2\nu + \delta$, $\nu \geqslant 0$, $\delta = 0, 1$, 或 z, 我们确定 Δ, 使得

$$\Delta = \begin{cases} \varnothing, & \text{如果}\, k = 2\nu \,\text{而}\, (-1)^\nu \xi \in \mathbb{F}_q^{*2}, \\ (1), \text{或}\, (z), & \text{如果}\, k = 2\nu + 1, \\ [1, -z], & \text{如果}\, k = 2\nu \,\text{而}\, (-1)^\nu \xi \in z\mathbb{F}_q^{*2}, \end{cases}$$

那么

$$\begin{aligned} p^{(k,\xi)}_{(i,\eta)(j,\zeta)}(n) = & \textstyle\sum_{0 \leqslant t \leqslant n-k,\, \rho=1,z} k_{(t,\rho)}(n-k) \\ & \textstyle\sum_{m,s,\gamma,\Gamma\,\text{满足}\,(5.23)} \displaystyle\prod_{i=n-k-t-m+1}^{n-k-t} (q^i - 1) q^{\frac{1}{2}m(m-1)} \\ & \cdot N(m,\, 2s+\gamma,\, s,\, \Gamma;\, 2\nu+\delta,\, \Delta) q^{kt + \frac{1}{2}m(2k+1-m)} \\ & \cdot p^{(k-2m+2s+\gamma,\xi')}_{(i-t-2m,\eta')\,(j-t-2m,\zeta')}(k-m), \end{aligned}$$

其中 $\xi' = 1$ 或 z 分别由 $(-1)^{\nu-m+s}\det(-\Gamma)\det\Delta \in \mathbb{F}_q^{*2}$ 或 $(-1)^{\nu-m+s}\det(-\Gamma) \cdot\det\Delta \in z\mathbb{F}_q^{*2}$ 来确定;$\eta' = 1$ 或 z 分别由 $\eta/(-1)^m\rho \in \mathbb{F}_q^{*2}$ 或 $\eta/(-1)^m\rho \in z\mathbb{F}_q^{*2}$ 来确定;$\zeta' = 1$, 或 z 分别由 $\zeta/(-1)^{m+t}\rho \in \mathbb{F}_q^{*2}$ 或 $\zeta/(-1)^{m+t}\rho \in z\mathbb{F}_q^{*2}$ 来确定.

§5.6 参数的计算续

下面给出 $p^{(n,\xi)}_{(n,\eta)(n,\zeta)'}(n)$ 的一种递推算法. 根据命题 1.1(vi), 我们只需讨论 $p^{(n,\xi)}_{(n,1)(n,1)'}(n)$ 和 $p^{(n,\xi)}_{(n,z)(n,z)'}(n)$.

设 $n \geqslant 3$. 先计算 $p^{(n,\xi)}_{(n,1)(n,1)'}(n)$. 我们取

$$S_1 = 0^{(n)},\ S_2 = \left[\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & \xi \end{pmatrix},\ I^{(n-3)}\right].$$

令

$$\mathcal{M}^{(n,\xi)}_{(n,1)(n,1)'} = \{S \in \mathcal{S}(n, q) | (S_1,\, S) \in R_{(n,1)},\ (S,\, S_2) \in R_{(n,1)'}\}.$$

显然

$$\mathcal{M}^{(n,\xi)}_{(n,1)(n,1)'} = \{S \in \mathcal{S}(n,q) | \det(S - S_i) \in \mathbb{F}_q^{*2},\ i = 1, 2\}.$$

令

$$\begin{aligned} \mathcal{M}_0 &= \{S = (s_{ij}) \in \mathcal{M}^{(n,\xi)}_{(n,1)(n,1)'} | s_{11} = 0\}, \\ \mathcal{M}_1 &= \{S = (s_{ij}) \in \mathcal{M}^{(n,\xi)}_{(n,1)(n,1)'} | s_{11} \neq 0\}. \end{aligned}$$

那么

$$p^{(n,\xi)}_{(n,1)\,(n,1)'}(n) = |\mathcal{M}^{(n,\xi)}_{(n,1),(n,1)'}| = |\mathcal{M}_0| + |\mathcal{M}_1|. \tag{5.41}$$

对于 $S \in \mathcal{M}^{(n,\xi)}_{(n,1)(n,1)'}$. 取 S 为分块矩阵

$$\begin{pmatrix} a & b & v_1 & v_2 \\ b & c & u_1 & u_2 \\ {}^t v_1 & {}^t u_1 & w_{11} & w_{12} \\ {}^t v_2 & {}^t u_2 & {}^t w_{12} & w_{22} \end{pmatrix} \begin{matrix} 1 \\ 1 \\ 1 \\ n-3 \end{matrix} \qquad (5.42)$$
$$\quad\;\; 1 \qquad 1 \qquad 1 \qquad n-3$$

我们引进 G 的子群 H, 它由形如

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ -\frac{1}{2}[\xi w\,{}^t w + w_1\,{}^t w_1] & 1 & -w & -w_1 \\ \xi\,{}^t w & 0 & 1 & 0 \\ {}^t w_1 & 0 & 0 & I^{(n-3)} \end{pmatrix}$$

的矩阵组成. 容易验证 H 作用在 $S(n,q)$ 上保持 S_1 和 S_2 不变, 从而把 $\mathcal{M}^{(n,-1)}_{(n,1)\,(n,1)'}$ 变成它自己. 进一步, 可知 H 保持 $\mathcal{M}_0$ 和 $\mathcal{M}_1$ 不变.

我们先计算 $|\mathcal{M}_1|$. 令 $u=(u_1, u_2)$, $W = \begin{pmatrix} w_{11} & w_{12} \\ {}^t w_{12} & w_{22} \end{pmatrix}$ 和

$$\mathcal{M}_1' = \left\{ \begin{pmatrix} a & b & 0 \\ b & c & u \\ 0 & {}^t u & W \end{pmatrix} \in \mathcal{M}_1 \right\},$$

对于 $S \in \mathcal{M}_1$, 而 S 取形如 (5.42) 的分块矩阵. 如果取

$$T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ v^* & 1 & a^{-1}\xi^{-1}v_1 & a^{-1}v_2 \\ -\xi\,{}^t(a^{-1}\xi^{-1}v_1) & 0 & 1 & 0 \\ -\,{}^t(a^{-1}v_2) & 0 & 0 & I^{(n-3)} \end{pmatrix} \in H,$$

这里 $v^* = -\frac{1}{2}[(a^{-1}v_2)\,{}^t(a^{-1}v_2) + \xi(a^{-1}\xi^{-1}v_1)\,{}^t(a^{-1}\xi^{-1}v_1)]$, 那么易知 $TS\,{}^tT \in \mathcal{M}_1'$, 从而得到

$$|\mathcal{M}_1| = q^{n-2}|\mathcal{M}_1'|. \qquad (5.43)$$

对于任意

$$S = \begin{pmatrix} a & b & 0 \\ b & c & u \\ 0 & {}^t u & W \end{pmatrix} \in \mathcal{M}_1',$$

S 和 $S-S_2$ 分别合同于

$$\left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & c-a^{-1}b^2 & u \\ 0 & {}^t u & W \end{pmatrix} \right\} \text{和} \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & c-a^{-1}(b-1)^2 & u \\ 0 & {}^t u & W-[\xi, I^{(n-3)}] \end{pmatrix} \right\}.$$

令

$$\widetilde{S}_1 = 0^{(n-1)},\ \widetilde{S}_2 = \begin{pmatrix} a^{-1}(1-2b) & 0 \\ 0 & [\xi, I^{(n-3)}] \end{pmatrix},\ \widetilde{S} = \begin{pmatrix} c - a^{-1}b^2 & u \\ {}^t u & W \end{pmatrix}.$$

从 $\det(S - S_i) \in \mathbb{F}_q^{*2}$, $i = 1, 2$, 我们得到

$$\widetilde{S} - \widetilde{S}_i \sim [I^{(n-2)}, \eta],\ \eta = \begin{cases} 1, & \text{如果}\, a \in \mathbb{F}_q^{*2}, \\ z, & \text{如果}\, a \notin \mathbb{F}_q^{*2} \end{cases}$$

和

$$\widetilde{S}_2 - \widetilde{S}_1 \sim \begin{cases} [I^{(n-3)}, \xi, 0], & \text{如果}\, 1 - 2b = 0, \\ [I^{(n-2)}, \xi], & \text{如果}\, a^{-1}(1-2b) \in \mathbb{F}_q^{*2}, \\ [I^{(n-2)}, \xi z], & \text{如果}\, a^{-1}(1-2b) \in z\mathbb{F}_q^{*2}. \end{cases}$$

因而

$$\begin{aligned} |\mathcal{M}_1'| = &\frac{1}{2}(q-1)\sum_{\eta=1,z} p^{(n-2,\xi)}_{(n-1,\eta)(n-1,\eta)'}(n-1) \\ &+ \frac{1}{4}(q-1)^2 \sum_{\xi',\eta=\xi,\xi z} p^{(n-1,\xi')}_{(n-1,\eta)(n-1,\eta)'}(n-1). \end{aligned}$$

(注意, 当 $\xi = z$ 时, 取 $\xi z = 1$.) 把上式代入 (5.43), 得

$$\begin{aligned} |\mathcal{M}_1| = \frac{1}{4}q^{(n-2)}\ \ (q-1)\Big\{&2\sum_{\eta=1,z} p^{(n-2,\xi)}_{(n-1,\eta)(n-1,\eta)'}(n-1) \\ &+(q-1)\sum_{\xi',\eta=\xi,\xi z} p^{(n-1,\xi')}_{(n-1,\eta)(n-1,\eta)'}(n-1)\Big\}. \end{aligned} \tag{5.44}$$

下面再来计算 $|\mathcal{M}_0|$. 令

$$S = \begin{pmatrix} 0 & b & v \\ b & c & u \\ {}^t v & {}^t u & W \end{pmatrix}$$

是 $\mathcal{M}_0$ 中的一个元素. 我们按照 $v = 0$, $v \neq 0$ 而 $v\,{}^t v = 0$, $v\,{}^t v \in \mathbb{F}_q^{*2}$, 或 $v\,{}^t v \in z\mathbb{F}_q^{*2}$, 分别把 $\mathcal{M}_0$ 划分成它的子集合 $\mathcal{M}_0'$, $\mathcal{M}_{00}$, $\mathcal{M}_{01}$ 和 $\mathcal{M}_{0z}$, 那么

$$|\mathcal{M}_0| = |\mathcal{M}_0'| + |\mathcal{M}_{00}| + |\mathcal{M}_{01}| + |\mathcal{M}_{0z}|. \tag{5.45}$$

注意到, 如果 $v \neq 0$ 而 $v\,{}^t v = 0$, $v\,{}^t v \in \mathbb{F}_q^{*2}$, 或 $v\,{}^t v \in z\mathbb{F}_q^{*2}$, 那么就把 v 称为迷向向量, 平方型的非迷向向量, 或非平方型的非迷向向量.

我们先来计算 $|\mathcal{M}_0'|$. 令

$$S = \begin{pmatrix} 0 & b & 0 \\ b & c & u \\ 0 & {}^t u & W \end{pmatrix} \in \mathcal{M}_0',$$

那么

$$\det S = -b^2 \det W,\ \det(S - S_2) = -(b-1)^2 \det(W - [\xi,\ I^{(n-3)}]).$$

因为 $\det(S - S_i) \in \mathbb{F}_q^{*2}$, $b \neq 0$, $b - 1 \neq 0$, 所以 $\det W$ 和 $\det(W - [\xi,\ I^{(n-3)}])$ 都属于 $(-1)\mathbb{F}_q^{*2}$. 令

$$\widetilde{S}_1 = 0^{(n-2)},\ \widetilde{S}_2 = [\xi, I^{(n-3)}],\ \widetilde{S} = W.$$

那么

$$\widetilde{S}_2 - \widetilde{S}_1 = [\xi, I^{(n-3)}],\ \widetilde{S} - \widetilde{S}_i \sim [I^{(n-3)}, -1],\ i = 1, 2.$$

(注意, 当 $q \equiv 1 (\mathrm{mod}\, 4)$ 时,$-1 \in \mathbb{F}_q^{*2}$, 所以 $M(n-2, n-2, -1) \sim M(n-2, n-2, 1)$; 当 $q \equiv 3 (\mathrm{mod}\, 4)$ 时,$-1 \in z\mathbb{F}_q^{*2}$, 所以 $M(n-2, n-2, -1) \sim M(n-2, n-2, z)$. 后面用到符号 $M(m, r, a), a = 1$ 或 z 时, 也应这样考虑). 因此

$$|\mathcal{M}_0'| = (q-2)q^{n-1} p^{(n-2,\xi)}_{(n-2,-1)\,(n-2,-1)'}(n-2). \tag{5.46}$$

其次, 我们来计算 $|\mathcal{M}_{0\alpha}|, \alpha = 0, 1,$ 或 z. 选取

$$v_\alpha = \underset{1}{(1} \quad \underset{n-3}{v_{\alpha 2})},$$

其中

$$v_{\alpha 2} = \begin{cases} (\lambda_1, \lambda_2, 0, \cdots, 0), & \text{如果}\, \alpha = 0, \text{这里}\, \lambda_1, \lambda_2 \in \mathbb{F}_q^* \\ & \text{使得}\, \xi + \lambda_1^2 + \lambda_2^2 = 0, \\ (0, 0, 0, \cdots, 0), & \text{如果}\, \alpha = \xi, \\ (\mu, 0, \cdots, 0), & \text{如果}\, \alpha = \xi z, \text{这里}\, \mu \in \mathbb{F}_q^* \\ & \text{使得}\, \xi + \mu^2 = \xi z. \end{cases}$$

再令

$$\mathcal{M}_{0\alpha}(v_\alpha) = \left\{ \begin{pmatrix} 0 & b & v_\alpha \\ b & c & u \\ {}^t v_\alpha & {}^t u & W \end{pmatrix} \in \mathcal{M}_{0\alpha} \right\},$$

我们引进 G 的另一子群 K, 它由形如

$$\begin{pmatrix} x & & \\ & x^{-1} & \\ & & T \end{pmatrix}$$

的矩阵组成, 其中 $x \in \mathbb{F}_q^*$ 而 $T[\xi, I^{(n-3)}]\,{}^tT = [\xi, I^{(n-3)}]$. 显然 K 保持 S_1 和 S_2 不变, 并且把 $\mathcal{M}_{0\alpha}$ 变成其自己 ($\alpha = 0, 1$, 或 z). 此外, 在 K 的作用下, $\mathcal{M}_{0\alpha}$ 的任一元素变成 $\mathcal{M}_{0\alpha}$ 的任一元素. 因此

$$|\mathcal{M}_{0\alpha}| = N_\alpha |\mathcal{M}_{0\alpha}(v_\alpha)|, \tag{5.47}$$

其中 N_0, N_1 和 N_z 分别是关于 $I^{(n-2)}$ 的迷向向量, 平方型迷向向量和非迷向向量的个数. 下面给出它们的计算公式.

令 $n-2 = 2\nu + \delta$, $\delta = 0, 1$, 或 2, 其中 ν 和 δ 的值确定如下:

当 $q \equiv 1 (\bmod 4)$ 时, 如果 $\xi = 1$, 那么

$$n-2=\begin{cases}2\nu,\\2\nu+1,\end{cases}\quad \delta=\begin{cases}0,\\1,\end{cases}\quad \Delta=\begin{cases}\varnothing, & \text{如果}\, n-2\equiv 0 \,(\bmod 2),\\ 1, & \text{如果}\, n-2\equiv 1\,(\bmod 2).\end{cases}$$

如果 $\xi = z$, 那么

$$n-2=\begin{cases}2\nu+2,\\2\nu+1,\end{cases}\quad \delta=\begin{cases}2,\\1,\end{cases}\quad \Delta=\begin{cases}[1,-z], & \text{如果}\, n-2\equiv 0 \,(\bmod 2),\\ z, & \text{如果}\, n-2\equiv 1\,(\bmod 2).\end{cases}$$

当 $q \equiv 3 (\bmod 4)$ 时, 如果 $\xi = 1$, 那么

$$n-2=\begin{cases}2\nu,\\2\nu+1,\\2\nu+1,\\2(\nu-1)+2,\end{cases}\quad \delta=\begin{cases}0,\\1,\\1,\\2,\end{cases}\quad \Delta=\begin{cases}\varnothing, & \text{如果}\, n-2\equiv 0 \,(\bmod 4),\\ 1, & \text{如果}\, n-2\equiv 1\,(\bmod 4),\\ z, & \text{如果}\, n-2\equiv 3\,(\bmod 4),\\ [1,-z], & \text{如果}\, n-2\equiv 2\,(\bmod 4).\end{cases}$$

如果 $\xi = z$, 那么

$$n-2=\begin{cases}2(\nu-1)+2,\\2\nu+1,\\2\nu+1,\\2\nu,\end{cases}\quad \delta=\begin{cases}2,\\1,\\1,\\0,\end{cases}\quad \Delta=\begin{cases}[1,-z], & \text{如果}\, n-2\equiv 0 \,(\bmod 4),\\ z, & \text{如果}\, n-2\equiv 1\,(\bmod 4),\\ 1, & \text{如果}\, n-2\equiv 3\,(\bmod 4),\\ \varnothing, & \text{如果}\, n-2\equiv 2\,(\bmod 4).\end{cases}$$

注意到 $2\nu + \delta$ 维正交空间中, 关于 $S_{2\nu+\delta,\Delta}$ 的 $(1, 0, 0, \varnothing)$, $(1, 1, 0, 1)$, $(1, 1, 0, z)$ 型子空间[15] 分别含有 $q-1$ 个不同的非零迷向向量, 平方型非迷向向量和非平方型非迷向向量. 因此由 [15] 定理 6.26, 可得

$$N_0 = (q^\nu - 1)(q^{\nu+\delta-1} + 1). \tag{5.48}$$

$$N_1 = \frac{1}{2}(q-1)\begin{cases}(q^\nu - 1)q^{\nu-1}, & \text{如果}\, \delta = 0,\\ (q^\nu + 1)q^\nu, & \text{如果}\, \delta = 1\, \text{而}\, \Delta = 1,\\ (q^\nu - 1)q^\nu, & \text{如果}\, \delta = 1\, \text{而}\, \Delta = z,\\ (q^\nu + 1)q^{\nu-1}, & \text{如果}\, \delta = 2,\end{cases} \tag{5.49}$$

$$N_z = \begin{cases} (q^\nu - 1)q^{\nu-1}, & \text{如果}\, \delta = 0, \\ (q^\nu - 1)q^\nu, & \text{如果}\, \delta = 1\, \text{而}\, \Delta = 1, \\ (q^\nu + 1)q^\nu, & \text{如果}\, \delta = 1\, \text{而}\, \Delta = z, \\ (q^\nu + 1)q^{\nu-1}, & \text{如果}\, \delta = 2. \end{cases} \tag{5.50}$$

剩下的工作主要是来计算 $|\mathcal{M}_{0\alpha}(v_\alpha)|$.

对于 $S_\alpha \in \mathcal{M}_{0\alpha}(V_\alpha)$, 我们把 S_α 写成分块矩阵形式

$$S_\alpha = \begin{pmatrix} 0 & b & 1 & v_{\alpha 2} \\ b & c & u_1 & u_2 \\ 1 & u_1 & w_{11} & w_{12} \\ {}^t v_{\alpha 2} & {}^t u_2 & {}^t w_{12} & w_{22} \end{pmatrix}. \tag{5.51}$$

令

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ w^* & 1 & \frac{w_{11}}{2}\xi^{-1} & w_{12} - \frac{w_{11}}{2} v_{\alpha 2} \\ -\frac{w_{11}}{2} & 0 & 1 & 0 \\ -{}^t(w_{12} - \frac{w_{11}}{2} v_{\alpha 2}) & 0 & 0 & I^{(n-3)} \end{pmatrix}, \tag{5.52}$$

其中 $w^* = -\frac{1}{2}[\frac{w_{11}^2 \xi^{-1}}{4} + (w_{12} - \frac{w_{11}}{2} v_{\alpha 2})\, {}^t(w_{12} - \frac{w_{11}}{2} v_{\alpha 2})]$. 要注意, 当 $n = 3$ 时, (5.51) 中的第四行, 第四列不出现, 而在 (5.52) 中, 第四行, 第四列也不出现. 那么在合同变换

$$S \longrightarrow PS\,{}^tP$$

下,S_1 和 S_2 保持不变, 而 S_α 变成形如

$$\begin{pmatrix} 0 & * & 1 & v_{\alpha 2} \\ * & * & * & * \\ 1 & * & 0 & 0 \\ {}^t v_{\alpha 2} & * & 0 & * \end{pmatrix}$$

的矩阵. 令

$$\mathcal{M}'_{0\alpha}(v_\alpha) = \left\{ \begin{pmatrix} 0 & b & 1 & v_{\alpha 2} \\ b & c & u_1 & u_2 \\ 1 & u_1 & 0 & 0 \\ {}^t v_{\alpha 2} & {}^t u_2 & 0 & w_{22} \end{pmatrix} \in \mathcal{M}_{0\alpha}(v_\alpha) \right\},$$

那么

$$|\mathcal{M}_{0\alpha}(v_\alpha)| = q^{n-2} |\mathcal{M}'_{0\alpha}(v_\alpha)|. \tag{5.53}$$

现在来计算 $|\mathcal{M}'_{0\alpha}|$. 令

$$S=\begin{pmatrix}0&b&1&v_{\alpha2}\\ b&c&u_1&u_2\\ 1&u_1&0&0\\ {}^tv_{\alpha2}&{}^tu_2&0&w_{22}\end{pmatrix}\in\mathcal{M}'_{0\alpha}(v_\alpha),$$

那么

$$\det S=(-1)\det\begin{pmatrix}c-2u_1b&u_2-u_1v_{\alpha2}\\ {}^tu_2-u_1\,{}^tv_{\alpha2}&w_{22}\end{pmatrix},$$

$$\det(S-S_2)=(-1)\det\left(\begin{pmatrix}(c-2u_1b&u_2-u_1v_{\alpha2}\\ {}^tu_2-u_1\,{}^tv_{\alpha2}&w_{22}\end{pmatrix}-\begin{pmatrix}\xi(b-1)^2-2u_1&\xi(b-1)v_{\alpha2}\\ \xi(b-1)\,{}^tv_{\alpha2}&\xi\,{}^tv_{\alpha2}v_{\alpha2}+I\end{pmatrix}\right).$$

令

$$\widetilde{S}_1=0^{(n-2)},\quad \widetilde{S}_2=\begin{pmatrix}\xi(b-1)^2-2u_1&\xi(b-1)v_{\alpha2}\\ \xi(b-1)\,{}^tv_{\alpha2}&\xi\,{}^tv_{\alpha2}v_{\alpha2}+I\end{pmatrix},$$

$$\widetilde{S}=\begin{pmatrix}c-2u_1b&u_2-u_1v_{\alpha2}\\ {}^tu_2-u_1\,{}^tv_{\alpha2}&w_{22}\end{pmatrix}.$$

从 $\det(S-S_i)\in\mathbb{F}_q^{*2}$ 得到 $\det(\widetilde{S}-\widetilde{S}_i)\in(-1)\mathbb{F}_q^{*2}$. 因而

$$\widetilde{S}-\widetilde{S}_i\sim[I^{(n-3)},-1]$$

或

$$(\widetilde{S}_i,\widetilde{S})\in R_{(n-2,-1)}(n-2).$$

然而, 要讨论 $(\widetilde{S}_1,\widetilde{S}_2)$ 所属的类, 需要对 $\alpha=0$, 1, 和 z 分别进行考虑.

我们取 $\alpha=0$ 作为例子, 这时经过计算可得

$$\det(\widetilde{S}_2-\widetilde{S}_1)=\det\begin{pmatrix}\xi(b-1)^2-2u_1&\xi(b-1)v_{02}\\ \xi(b-1)\,{}^tv_{02}&\xi\,{}^tv_{02}v_{02}+I\end{pmatrix}=\xi(b-1)^2.$$

对于 $b=1$,

$$\widetilde{S}_2-\widetilde{S}_1\sim\begin{pmatrix}-2u_1&0&0&0\\ 0&0&0&0\\ 0&0&I^{(n-5)}&0\\ 0&0&0&-\xi\end{pmatrix}.$$

于是

$$\widetilde{S}_2-\widetilde{S}_1\sim\begin{cases}[I^{(n-5)},-\xi,0^{(2)}], & \text{如果}\ u_1=0,\\ [I^{(n-4)},-\xi,0], & \text{如果}\ -2u_1\in\mathbb{F}_q^{*2},\\ [I^{(n-4)},-z\xi,0], & \text{如果}\ -2u_1\in z\mathbb{F}_q^{*2}.\end{cases}$$

而对应于上述三种情形,$\widetilde{S}_2$ 分别有 1, $\frac{1}{2}(q-1)$ 和 $\frac{1}{2}(q-1)$ 种选取. 对于 $b \neq 1$.

$$\widetilde{S}_2 - \widetilde{S}_1 \sim [I^{(n-3)}, \xi],$$

而 $\widetilde{S}_2$ 有 $q(q-1)$ 种选取, 因此

$$\begin{aligned}|\mathcal{M}'_{00}(V_0)| = & \; p^{(n-4,-\xi)}_{(n-2,-1)(n-2,-1)}(n-2) \\ & +\frac{1}{2}(q-1)\sum_{\xi'=\xi,\xi z} p^{(n-3,\xi')}_{(n-2,-1)(n-2,-1)'}(n-2) \\ & +q(q-1)p^{(n-2,\xi)}_{(n-2,-1)(n-2,-1)'}(n-2).\end{aligned} \tag{5.54}$$

类似地, 我们有

$$\begin{aligned}|\mathcal{M}'_{01}(v_1)| = & \; qp^{(n-3,1)}_{(n-2,-1)(n-2,-1)'}(n-2) \\ & +\frac{1}{2}q(q-1)\sum_{\xi'=1,z} p^{(n-2,\xi')}_{(n-2,-1)(n-2,-1)'}(n-2),\end{aligned} \tag{5.55}$$

$$\begin{aligned}|\mathcal{M}'_{0z}(v_2)| = & \; qp^{(n-3,\tau)}_{(n-2,-1)(n-2,-1)'}(n-2) \\ & +\frac{1}{2}q(q-1)\sum_{\xi'=1,z} p^{(n-2,\xi')}_{(n-2,-1)(n-2,-1)'}(n-2),\end{aligned} \tag{5.56}$$

这里

$$\tau = \begin{cases} \xi, & 如果\, 1-\dfrac{1}{z} \in \mathbb{F}_q^{*2}, \\ z\xi, & 如果\, 1-\dfrac{1}{z} \in z\mathbb{F}_q^{*2}. \end{cases} \tag{5.57}$$

从 (5.41), (5.44)~(5.47), (5.53)~(5.55) 和 (5.56) 就得到

定理 5.12 $n \geqslant 3$ 时, n 阶对称矩阵结合方案 $\mathrm{Sym}(n,q)$ 的交叉数

$$\begin{aligned}p^{(n,\xi)}_{(n,1)(n,1)'}(n) = & \; q^{(n-2)}\Big\{\frac{1}{2}(q-1)\sum_{\eta=1,z} p^{(n-2,\xi)}_{(n-1,\eta)(n-1,\eta)'}(n-1) \\ & +\frac{1}{4}(q-1)^2\sum_{\eta,\xi'=1,z} p^{(n-1,\xi')}_{(n-1,\eta)(n-1,\eta)'}(n-1)\Big\} \\ & +[q(q-2)+q(q-1)N_0]p^{(n-2,\xi)}_{(n-2,-1)(n-2,-1)'}(n-2) \\ & +N_0\Big[p^{(n-4,-\xi)}_{(n-2,-1)(n-2,-1)'}(n-2) \\ & +\frac{1}{2}(q-1)\sum_{\xi'=1,z} p^{(n-3,1)}_{(n-2,-1)(n-2,-1)'}(n-2)\Big] \\ & +qN_1p^{(n-3,1)}_{(n-2,-1)(n-2,-1)'}(n-2)+qN_zp^{(n-3,\tau)}_{(n-2,-1)(n-2,-1)'}(n-2) \\ & +\frac{1}{2}q(q-1)(N_1+N_z)\sum_{\xi'=1,z} p^{(n-2,\xi')}_{(n-2,-1)(n-2,-1)'}(n-2),\end{aligned} \tag{5.58}$$

这里 τ 由 (5.57) 确定.

按照定理 5.12 的推导步骤, 同样可得

定理 5.13 $n \geqslant 3$ 时, n 阶对称矩阵结合方案 $\mathrm{Sym}(n,q)$ 的交叉数

$$
\begin{aligned}
p^{(n,\xi)}_{(n,z)(n,z)'}(n) =& q^{(n-2)}\Big\{\frac{1}{2}(q-1)\sum_{\eta=1,z} p^{(n-2,\xi)}_{(n-1,\eta)(n-1,\eta)'}(n-1) \\
&+\frac{1}{4}(q-1)^2\sum_{\eta,\xi'=1,z} p^{(n-1,\xi')}_{(n-1,\eta)(n-1,\eta)'}(n-1)\Big\} \\
&+[q(q-2)+q(q-1)N_0]p^{(n-2,\xi)}_{(n-2,-z)(n-2,-z)'}(n-2) \\
&+N_0\Big[p^{(n-4,-\xi)}_{(n-2,-z)(n-2,-z)'}(n-2) \\
&+\frac{1}{2}(q-1)\sum_{\xi'=\xi,\xi z} p^{(n-3,1)}_{(n-2,-z)(n-2,-z)'}(n-2)\Big] \\
&+qN_1 p^{(n-3,1)}_{(n-2,-z)(n-2,-z)'}(n-2)+qN_z p^{(n-3,\tau)}_{(n-2,-z)(n-2,-z)'}(n-2) \\
&+\frac{1}{2}q(q-1)(N_1+N_z)\sum_{\xi'=1,z} p^{(n-2,\xi')}_{(n-2,-z)(n-2,-z)'}(n-2), \qquad (5.59)
\end{aligned}
$$

这里 τ 由 (5.57) 确定.

§5.7 结合方案 Quad(n, q)

设 $\mathcal{X}=(X,\{R_i\}_{0\leqslant i\leqslant d})$ 和 $\mathcal{Y}=(Y,\{R'_j\}_{0\leqslant j\leqslant d'})$ 是两个结合方案, 如果 $Y=X$, 并且 $\mathcal{Y}$ 的每个结合类 R'_j 都是 $\mathcal{X}$ 的结合类之并, 那么, 就说 $\mathcal{Y}$ 是 $\mathcal{X}$ 的一个聚合 (fusion) 方案, 也说 $\mathcal{X}$ 是 $\mathcal{Y}$ 的一个分裂 (fission) 方案. 例如,1.1 中提到的非对称交换结合方案 $\mathcal{X}$ 的对称化 $\overline{\mathcal{X}}$ 就是 $\mathcal{X}$ 的一个聚合方案, 我们有下面一个具体例子.

设 $q\equiv 3 \pmod 4$, 这时 -1 不是平方元,$\mathbb{F}_q$ 上秩为奇数 $2s+1$ 的 $n\times n$ 对称矩阵确定的结合类 $R_{(2s+1,\xi)}(n)$, ($\xi=1$ 或 z) 不是对称的, 而有下面的的关系:

$$
R'_{(2s+1,1)}=R_{(2s+1,z)}(n),\ R'_{(2s+1,z)}=R_{(2s+1,1)}(n),\quad 0\leqslant s\leqslant\Big[\frac{n-1}{2}\Big].
$$

这时结合方案 $\mathrm{Sym}(n,q)$ 不是对称的. 注意到, 对于秩为偶数 $2s$ 的对称矩阵确定的结合类 $R_{(2s,\xi)}$ 都是对称的, 即 $R'_{(2s,\xi)}=R_{(2s,\xi)}$, ($\xi=1$ 或 z).

现在, 对于奇数 $2s+1$, 令 $\widetilde{R}_{2s+1}=R_{(2s+1,1)}(n)\cup R_{(2s+1,z)}(n)\,(0\leqslant s\leqslant[\frac{n-1}{2}])$; 而对于偶数 $2s$, 令 $\widetilde{R}_{2s}=R_{(2s,1)}(n)$, $\widetilde{R}_{n+s}=R_{(2s,z)}(n)\,(0\leqslant s\leqslant[\frac{n}{2}])$. 那么, 当 $q\equiv 3 (\mathrm{mod}\ 4)$ 时,$\mathrm{Sym}(n,q)$ 的对称化就是

$$
\widetilde{\mathrm{Sym}}(n,q)=(X_n,\{\widetilde{R}\}_{0\leqslant i\leqslant n+[\frac{n}{2}]}).
$$

它是 $\mathrm{Sym}(n,q)$ 的一个聚合方案.

值得注意的是, 当 $q\equiv 1 (\mathrm{mod}\, 4)$ 时, 如上构作结合类却不能形成结合方案. 按秩确定结合关系也不能形成结合方案.

Y.Egawa 在 $\mathbb{F}_q$ 上 n 元二次型的集合上定义了一个结合方案, 其中 q 为任意素数 p 的幂 ([4]). 我们知道, 当 $p \neq 2$ 时,$\mathbb{F}_q$ 上的 n 元二次型与 $\mathbb{F}_q$ 上的 $n \times n$ 对称矩阵一一对应. 这时, 这个结合方案是 $\mathrm{Sym}(n, q)$ 的一个聚合方案. 本节介绍 $p \neq 2$ 时的情形. 关于 $p = 2$ 时的情形将在第七章中介绍.

令 $X_n = S(n, q)$, 即 $\mathbb{F}_q$ 上全体 $n \times n$ 对称矩阵的集合. 令

$$\overline{R}_i = \{(X, Y)|X, Y \in X_n, \operatorname{rank}(X - Y) = 2i - 1 \text{或} 2i\} \left(0 \leqslant i \leqslant \left[\frac{n+1}{2}\right]\right).$$

[4] 中证明了 $(X_n, \{\overline{R}\}_{0\leqslant i\leqslant[\frac{n+1}{2}]})$ 是一个对称结合方案, 并且是 P 多项式的, 记作 $\mathrm{Quad}(n, q)$. 注意到, 对于 $i \in \{0, 1, \cdots, [\frac{n+1}{2}]\}$, $\overline{R}_i$ 为 $\mathrm{Sym}(n, q)$ 中如下结合类之并:

$$\overline{R}_i = R_{(2i-1,1)}(n) \cup R_{(2i-1,z)}(n) \cup R_{(2i,0)}(n) \cup R_{(2i,2)}(n),$$

因此 $\mathrm{Quad}(n, q)$ 是 $\mathrm{Sym}(n, q)$ 的一个聚合方案. 证明的关键是下面的

引理 5.14　对于 $i, j \in \{0, 1, \cdots, [\frac{n+1}{2}]\}$,

$$p_{i,1,j} := |\{S \in X_n|(S_1, S) \in \overline{R}_1, (S, S_2) \in \overline{R}_i\}|$$

是常数, 只要 $(S_1, S_2) \in \overline{R}_j$, 这里

(i) $p_{i,1,j} = 0$, 如果$|i - j| > 1$,

(ii) $p_{i-1,1,i} = \frac{q^{2i-2}(q^{2i}-1)}{q^2-1}$,

(iii) $p_{i,1,i} = \frac{(q^{2i}-1)(q^{n+1}+q^n-q^{2i}-q^{2i-2}-1)}{q^2-1}$,

(iv) $p_{i+1,1,i} = \frac{q^{4i}(q^{n-2i}-1)(q^{n-2i+1}-1)}{q^2-1}$.

证明　由于 $S(n, q)$ 作为加法群的平移群保持两个对称矩阵之差不变, 不失一般性, 我们可设 $S_1 = 0$, 而 S_2 为 $(2j-1, \xi)$ 型的,$\xi = 1$ 或 z, 或为 $(2j, \xi)$ 型的,$\xi = 0$ 或 2. 记 $\operatorname{rank} S_2 = k$, 这里 $k = 2j - 1$ 或 $2j$.

对于每个取定的型为 (k, ξ) 的 S_2, 我们能够计算出下面的数值

$$N_1 = |\{S \in X_n|\operatorname{rank} S = 1, \operatorname{rank}(S - S_2) = h\}|$$

和

$$N_2 = |\{S \in X_n|\operatorname{rank} S = 2, \operatorname{rank}(S - S_2) = h\}|,$$

其中 $h = 2m - 3, 2m - 2, 2m + 1$ 或 $2m + 3$. 对于 $k = 2m - 1$ 和 $k = 2m$ 时所得结果分别列成下面的表 5.3 和表 5.4.

表 5.3 S_2 的型为 $(2m-1, \xi)$ 时 N_1 和 N_2 的值

rank $(S_1 - S_2)$	rank $S = 2$	rank $S = 1$
$2m-3$	$\dfrac{q^{2m-2}(q^{2m-2}-1)}{q^2-1}$	0
$2m-2$	$q^{2m-2}(q^{2m-2}-1)$	q^{2m-2}
$2m+1$	$\dfrac{q^{4m}(q^{n-2m}-1)(q^{n-2m+1}-1)}{q^2-1}$	0
$2m+2$	0	0

表 5.4 S_2 的型为 $(2m, \xi)$ 时 N_1 和 N_2 的值

rank $(S_1 - S_2)$	rank $S = 2$	rank $S = 1$
$2m-3$	0	0
$2m-2$	$\dfrac{q^{2m-2}(q^{2m}-1)}{q^2-1}$	0
$2m+1$	$q^{2m}(q^{n-2m}-1)(q^{2m}-1)$	$q^{2m}(q^{n-2m}-1)$
$2m+2$	$\dfrac{q^{4m+2}(q^{n-2m}-1)(q^{n-2m-1}-1)}{q^2-1}$	0

这些数值的计算过程是比较冗长的, 我们将在下面作为例子给出两个数值的计算. 虽然在计算过程中涉及到矩阵的类型, 但结果却仅与秩有关.

本引理中 (i) 的证明是容易的, 因为对于任意三个矩阵 S_1, S_2, S_3, 下面的三角形不等式成立: rank$(S_1 - S_2)$+rank$(S_2 - S_3)$ $\geqslant$rank$(S_1 - S_2)$.

又, $p_{i-1,1,i}$ 为表 5.3 和表 5.4 前两行中结果之和, $p_{i+1,1,i}$ 为这两个表的后两行中结果之和, 它们与 $k = 2m - 1$ 或 $k = 2m$ 无关.

至于 $p_{i,1,i}$, 可由下面的等式导出:

$$
\begin{aligned}
& p_{i-1,1,i} + p_{i,1,i} + p_{i+1,1,i} = |\{S \in X_n | \operatorname{rank} S = 1 \text{ 或 } 2\}| \\
= & \textstyle\sum_{\xi=1,z} k_{(1,\xi)}(n) + \sum_{\xi=0,2} k_{(2,\xi)}(n) = \dfrac{(q^{n+1}-1)(q^n-1)}{q^2-1}.
\end{aligned} \tag{5.60}
$$

现在, 作为例子, 我们先来计算表 5.3 中第一列第一个数值, 即 $k = 2m-1, \xi = 1$ 或 z, 而 $h = 2m - 3$ 时的 N_2, 然后计算表 5.4 中第一列的第三个数值, 即 $k = 2m, \xi = 0$ 或 2, 而 $h = 2m - 2$ 时的 N_2. 采用结合方案 Sym(n, q) 的交叉数的概念. 如果 $[I^{(l-1)}, \rho] \sim S_{2s_0+\gamma_0,\Gamma_0}, [I^{k-1}, \xi] \sim S_{2s_1+\gamma_1,\Gamma_1}, [I^{(i-1)}, \eta] \sim S_{2s_2+\gamma_2,\Gamma_2}$ 和 $[I^{(j-1)}, \zeta] \sim S_{2s_3+\gamma_3,\Gamma_3}$, 其中对于 $i = 0, 1, 2, 3$,

$$
\Gamma_i = \begin{cases} \varnothing, & \text{如果 } \gamma_i = 0, \\ 1\text{或}z, & \text{如果 } \gamma_i = 1, \\ [1, -z], & \text{如果 } \gamma_i = 2, \end{cases}
$$

并且在 $\Gamma_i = \varnothing, 1, z$, 或 $[1, -z]$ 时, 分别取 $\Gamma_i' = 0, 1, z$, 或 2, 那么就令

$$k_{(l,\rho)}(n) = k_{(2s_0+\gamma_0,\Gamma_0')}(n),\ p_{(i,\eta)(j,\zeta)}^{(k,\xi)}(n) = p_{(2s_2+\gamma_2,\Gamma_2')(2s_3+\gamma_3,\Gamma_3')}^{(2s+\gamma_1,\Gamma_1')}(n).$$

我们先计算表 5.3 中第一列的第一个数值, 这就需要计算下面 4 个交叉数之和.

$$\sum_{\zeta=1,\,z} p_{(2,0)(2m-3,\,\zeta)}^{(2m-1,\,\xi)}(n) + \sum_{\zeta=1,\,z} p_{(2,2)(2m-3,\,\zeta)}^{(2m-1,\,\xi)}(n).$$

为了计算方便, 我们利用参数关系式

$$p_{(2,0)(2m-3,\,\zeta)}^{(2m-1,\,\xi)}(n) = \frac{k_{(2,0)}(n)}{k_{(2m-1,\,\xi)}(n)} p_{(2m-1,\,\xi)(2m-3,\,\zeta')}^{(2,0)}(n),$$

$$p_{(2,2)(2m-3,\,\zeta)}^{(2m-1,\,\xi)}(n) = \frac{k_{(2,2)}(n)}{k_{(2m-1,\,\xi)}(n)} p_{(2m-1,\,\xi)(2m-3,\,\zeta')}^{(2,2)}(n),$$

改为计算 $p_{(2m-1,\,\xi),\,(2m-3,\,\zeta)}^{(2,0)}(n)$ 和 $p_{(2m-1,\,\xi)(2m-3,\,\zeta)}^{(2,2)}(n)$. 记

$$p_{(2m-1,\,\xi),\,2m-3}^{(2,0)}(n) = \textstyle\sum_{\zeta=1,\,z} p_{(2m-1,\,\xi)(2m-3,\,\zeta)}^{(2,0)}(n)\,,$$

$$p_{(2m-1,\,\xi),\,2m-3}^{(2,2)}(n) = \textstyle\sum_{\zeta=1,\,z} p_{(2m-1,\,\xi)(2m-3,\,\zeta)}^{(2,2)}(n)\,.$$

先计算 $p_{(2m-1,\,\xi),\,2m-3}^{(2,0)}$. 取 $S_1 = 0$, $S_2 = \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ 0^{(n-2)}\right]$. 设 $S \in X_n$, 它的型为 $(2m-1, \xi)$, 而使得 $\operatorname{rank}(S - S_2) = 2m-3$. 将 S 按 S_2 的形状分块 $S = \begin{pmatrix} U & V \\ V' & W \end{pmatrix}$. 设 W 的型为 (t, ρ). 那么存在合同变换使 S_1 和 S_2 不变而将 S 变为

$$\begin{pmatrix} U & 0 & V \\ 0 & W_{(t,\,\rho)} & 0 \\ {}^tV & 0 & 0 \end{pmatrix} \begin{matrix} 2 \\ t \\ n-2-t \end{matrix}.$$

区分 $V = 0$ 和 $V \neq 0$ 两种情形讨论之.

(1) $V = 0$. 如果 $\operatorname{rank} U \leqslant 1$, 那么 $t = 2m-1$ 或 $2m-2$ 而 $\operatorname{rank}(S-S_2) > 2m-3$, 这种情形是不可能的. 所以 $\operatorname{rank} U = 2$, 而 $t = 2m-3$. 再由 $\operatorname{rank}(S - S_2) = 2m-3$, 推得 $U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, 这样 $-\rho \sim \xi$. 这时, 满足条件的 S 之个数为 $k_{(2m-3,\,\rho)}(n-2) \cdot q^{2(2m-3)}$.

(2) $V \neq 0$, 那么 $\operatorname{rank} V = 1$ 或 2, $t = 2m-5$ 或 $2m-3$, 但 $\operatorname{rank}(S-S_2) \geqslant 2m-1$, 这种情形不可能发生.

这样我们得到 $p_{(2m-1,\,\xi),\,2m-3}^{(2,0)}(n) = k_{(2m-3,\,\rho)}(n-2) \cdot q^{2(2m-3)}$.

同样的讨论可得到

$$p^{(2,\,2)}_{(2m-1,\,\xi),\,2m-3}(n) = k_{(2m-3,\,\rho')}(n-2)\cdot q^{2(2m-3)}.$$

这样, 在 $k=2m-1(\xi=1$ 或 $z)$ 和 $h=2m-3$ 时,

$$N_2 = \frac{k_{(2,\,0)}(n)}{k_{(2m-1,\,\xi)}(n)}\cdot k_{(2m-3,\,\rho)}(n-2)\cdot q^{4m-6} + \frac{k_{(2,\,2)}(n)}{k_{(2m-1,\,\xi)}(n)}\cdot k_{(2m-3,\,\rho')}(n-2)\cdot q^{4m-6}.$$

利用前面给出的计数公式求得 $N_2 = \frac{q^{2m-2}(q^{2m-2}-1)}{q^2-1}$.

现在来计算表 5.4 中第一列的第三个数值, 因为 $q\equiv 1(\mathrm{mod}\ 4)$ 和 $q\equiv 3(\mathrm{mod}\ 4)$ 时的计算方法相同, 所以在这里只给出 $q\equiv 1(\mathrm{mod}\ 4)$ 的计算. 按照上面计算表 5.3 中第一列第一个数值的步骤进行, 需要计算下列的参数

$$p^{(2m,\,0)}_{(2,\,0)(2m+1,\,1)}(n),\quad p^{(2m,\,0)}_{(2,\,0)(2m+1,\,z)}(n),\quad p^{(2m,\,0)}_{(2,\,2)(2m+1,\,1)}(n),\quad p^{(2m,\,0)}_{(2,\,2)(2m+1,\,z)}(n),$$

$$p^{(2m,\,2)}_{(2,\,0)(2m+1,\,1)}(n),\quad p^{(2m,\,2)}_{(2,\,0)(2m+1,\,z)}(n),\quad p^{(2m,\,2)}_{(2,\,2)(2m+1,\,1)}(n),\quad p^{(2m,\,2)}_{(2,\,2)(2m+1,\,z)}(n).$$

这些参数要通过分别计算下列参数

$$\begin{aligned}
&p^{(2,\,0)}_{(2m+1,\,1)(2m,\,0)}(n), && p^{(2,\,0)}_{(2m+1,\,z)(2m,\,0)}(n)\\
&p^{(2,\,2)}_{(2m+1,\,1)(2m,\,0)}(n), && p^{(2,\,2)}_{(2m+1,\,z)(2m,\,0)}(n),\\
&p^{(2,\,0)}_{(2m+1,\,1)(2m+2,\,2)}(n), && p^{(2,\,0)}_{(2m+1,\,z)(2m,\,2)}(n),\\
&p^{(2,\,2)}_{(2m+1,\,1)(2m,\,2)}(n), && p^{(2,\,2)}_{(2m+1,\,z)(2m,\,2)}(n)
\end{aligned}$$

和参数

$$k_{(2,\,0)}(n),\ k_{(2m,\,0)}(n),\ k_{(2,\,2)}(n),\ k_{(2m,\,2)}(n),$$

再利用命题 1.1(vi) 来实现.

(I) $p^{(2m,\,0)}_{(2,\,0)(2m+1,\,1)}(n)$ 和 $p^{(2m,\,0)}_{(2,\,0)(2m+1,\,z)}(n)$ 的计算.

先计算 $p^{(2m,\,0)}_{(2,\,0)(2m+1,\,1)}(n)$. 设 $S_1=0,\ \ S_2=\left[\begin{pmatrix}0&1\\1&0\end{pmatrix},\ 0^{(n-2)}\right]$ 和

$$\mathcal{M} = \{S\in S(n,\ q)|S\sim[S_{2m+1,\,1},\ 0^{(n-2m-1)}]\}. \tag{5.61}$$

当 S 遍及 $\mathcal{M}$ 时, 考察 $S-S_2$ 的变化范围, 进一步得到值 $p^{(2,\,0)}_{(2m+1,\,1)(2m,\,0)}(n)$, 从而得到 $p^{(2m,\,0)}_{(2,\,0)(2m+1,\,1)}(n)$.

设 $S \in \mathcal{M}$. 我们按照 (5.29) 到 (5.33) 的步骤进行, 把 S 变成

$$S = \begin{pmatrix} U & 0 & V \\ 0 & M_{(2t+\gamma,\Gamma)} & 0 \\ {}^tV & 0 & 0 \end{pmatrix} \begin{matrix} 2 \\ 2t+\gamma \\ n-2t-\gamma-2 \end{matrix}, \tag{5.62}$$
$$\qquad\quad \begin{matrix} 2 & \quad 2t+\gamma & \quad n-2t-\gamma-2 \end{matrix}$$

其中 $M_{(2t+\gamma,\Gamma)} \sim \left[\begin{pmatrix} 0 & I^{(t)} \\ I^{(t)} & 0 \end{pmatrix}, \Gamma\right]$, $\Gamma = \varnothing, 1, z$ 或 $[1, -z]$. 令 $\mathcal{M}_{(2t+\gamma,\Gamma)}$ 是 $\mathcal{M}$ 中形如 (5.62) 的所有矩阵组成的集合, 那么

$$|\mathcal{M}| = \sum_t k_{(2t+\gamma,\Gamma)}(n-2)q^{2(2t+\gamma)}|\mathcal{M}_{(2t+\gamma,\Gamma)}|. \tag{5.63}$$

现在对 $M_{(2t+\gamma,\Gamma)}$ 中 γ, Γ 的各种情形分别进行讨论.

(i) $\gamma = 0$. 再考察 V 的各种情形.

(i-a) $V = 0$, 这时 $t = m$, $U \sim [1, 0]$. 所以

$$S - S_2 \sim [S_{2m,\varnothing}, 0^{(n-2m)}] \tag{5.64}$$

不成立.

(i-b) $\operatorname{rank} V = 1$. 这时 $t = m-1$, V 是秩为 1 的 $2 \times (n-2m)$ 的矩阵. 所以存在 $(n-2m) \times (n-2m)$ 非奇异矩阵 Q, 使得 $VQ = \begin{pmatrix} \lambda & 0 & \cdots & 0 \\ \mu & 0 & \cdots & 0 \end{pmatrix}$, λ, μ 不全为 0. 当 $\lambda\mu \neq 0$ 时, 这样 V 的个数是 $(q-1)(q^{n-2m}-1)$; 当 $\lambda = 0$, 或 $\mu = 0$ 时, 上述 V 的个数分别是 $(q^{n-2m}-1)$.

由于 $[I^{2m}, Q]$ 作用 S_1, S_2 不动, 而把 (5.62) 变成

$$\begin{pmatrix} U & 0 & \begin{pmatrix} 1 & 0 & \cdots & 0 \\ \mu' & 0 & \cdots & 0 \end{pmatrix} \\ 0 & M_{(2(m-1),\varnothing)} & 0 \\ \begin{pmatrix} 1 & \mu' \\ 0 & 0 \\ \vdots & \vdots \\ 0 & 0 \end{pmatrix} & 0 & 0 \end{pmatrix}. \tag{5.65}$$

仍记 μ' 为 μ. 令 $U = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$, 那么

$$\begin{vmatrix} a & b & 1 \\ b & c & \mu \\ 1 & \mu & 0 \end{vmatrix} = 2b\mu - c - a\mu^2.$$

令 $c^* = 2b\mu - c - a\mu^2$, 那么

$$\begin{vmatrix} a & b-1 & 1 \\ b-1 & c & \mu \\ 1 & \mu & 0 \end{vmatrix} = c^* - 2\mu.$$

由 $S \sim [S_{2m+1,\,1},\, 0^{(n-2m-1)}]$, 有 $c^* \sim 1$, 并且在 $c^* = 2\mu$ 时,(5.64) 式成立, 而在 $c^* \neq 2\mu$ 时,(5.64) 不成立.

因为 $c^* \sim 1$ 的 c^* 的个数 $\frac{q-1}{2}$, 所以 2μ 的选取个数是 $\frac{q-1}{2}$. 因而满足 $c^* = 2\mu$ 的上述矩阵 V 的个数是 $\frac{1}{2}(q-1)(q^{n-2m}-1)$. 当 c^* 取定后,$(a,\, b,\, c)$ 的选取个数是 q^2. 所以当 $\lambda\mu \neq 0$ 时, 在 $\mathcal{M}(2(m-1),\, \varnothing)$ 中满足 (5.64) 的 S 的个数是

$$\frac{1}{2}(q-1)(q^{n-2m}-1)q^2. \tag{5.66}$$

当 $\mu = 0$ 或 $\lambda = 0$ 时,(5.64) 不成立.

(i-c) rank$V = 2$, 由 $S \sim [S_{2m+1,\,1},\, 0^{(n-2m-1)}]$, 可知这种情形不出现.

(ii) $\gamma = 1, \Gamma = 1$. 仍对 V 的各种情形进行考察.

(ii-a) $V = 0$. 这时 $t = m$ 或 $m-1$. 当 $t = m$ 时, 有 $U = 0$, 那么 (5.64) 不成立; 当 $t = m-1$ 时, 有 $U \sim \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. 如果

$$U - \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \sim [-1,\, 0], \tag{5.67}$$

那么 (5.64) 成立, 否则 (5.64) 不成立. 而满足 (5.67) 的 U 的个数是

$$p^{(2,\,0)}_{(2,\,0)(1,\,1)}(2) = \frac{1}{4}(q^2-1). \tag{5.68}$$

从而在 $\mathcal{M}(2(m-1)+1,\, 1)$ 中满足 (5.64) 的 S 的个数是 $\frac{1}{4}(q^2-1)$.

(ii-b) rank $V = 1$, 这时 $t = m-1$, 我们可取 $V = \begin{pmatrix} \lambda & 0 & \cdots & 0 \\ \mu & 0 & \cdots & 0 \end{pmatrix}$. 再按照 (i-b) 的推导进行, 可知在所考虑的情形,(5.64) 都不成立.

(ii-c) rank$V = 2$, 这时,$t = m-2$, 并且存在 $(n-2m+1) \times (n-2m+1)$ 非奇异矩阵 Q 使得 $VQ = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \end{pmatrix}$. $[I^{(2m-1)},\, Q]$ 作用 S_1 和 S_2 不变, 而把 (5.62)

变成

$$\begin{pmatrix} U & 0 & \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \end{pmatrix} \\ 0 & M_{(2(m-2)+1,\,1)} & 0 \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ \vdots & \vdots \\ 0 & 0 \end{pmatrix} & 0 & 0 \end{pmatrix}.$$

但 (5.64) 式不成立.

(iii) $\gamma = 1, \Gamma = z$. 再对 V 的各种情形进行考察.

(iii-a) $V = 0$. 这时 $t = m-1$, $U \sim [1, -z]$. 如果

$$U - \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \sim [-z, 0], \tag{5.69}$$

则 (5.64) 式成立, 否则 (5.64) 不成立, 而满足 (5.69) 的 U 的个数是

$$p^{(2,0)}_{(2,2)(1,z)}(2) = \frac{1}{4}(q-1)^2. \tag{5.70}$$

从而在 $\mathcal{M}(2(m-1)+1, z)$ 中满足 (5.69) 的 S 的个数是 $\frac{1}{4}(q-1)^2$.

(iii-b) $\text{rank}V = 1$, 按照 (i-b) 的推导, 可知这种情形不出现.

(iii-c) $\text{rank}V = 2$, 按照 (ii-c) 的推导, 可知这种情形也不出现.

(iv) $\gamma = 2, \Gamma = [1, -z]$. 再考察 V 的各种情形.

(iv-a) $V = 0$. 这时 $t = m-1$, $U \sim [z, 0]$, 易知 (5.64) 不成立.

(iv-b) rank $V = 1$, 这时 $t = m-2$, 我们可取 $V = \begin{pmatrix} \lambda & 0 & \cdots & 0 \\ \mu & 0 & \cdots & 0 \end{pmatrix}$, λ, μ 不全为 0, 如同 (i-b) 的推导, 可知 (5.64) 不成立.

(iv-c) $\text{rank}V = 2$, 由 $S \sim [S_{2m+1,1}, 0^{(n-2m-1)}]$, 可知这种情形不出现.

综上所述, 通过考察各种情形中 $S - S_2$ 的合同形式, 只有在 $S - S_2 \sim [S_{2m,\varnothing}, 0^{(n-2m)}]$ 时, 才满足要求.

根据 (5.63), 情形 (i-b), 情形 (ii-a) 和情形 (iii-a), 再考虑到 (5.66), (5.68) 和 (5.70), 有

$$\begin{aligned} p^{(2,0)}_{(2m+1,1)(2m,0)}(n) = & k_{(2(m-1)+1,1)}(n-2)q^{4m-2} \cdot \frac{1}{4}(q^2-1) \\ & + k_{(2(m-1)+1,z)}(n-2)q^{4m-2} \cdot \frac{1}{4}(q-1)^2 \\ & + k_{(2(m-1)),0)}(n-2)q^{4m-4} \cdot \frac{1}{2}(q-1)(q^{n-2m}-1)q^2. \end{aligned} \tag{5.71}$$

由定理 5.10,

$$k_{(2(m-1)+1,1)}(n-2)=k_{(2(m-1)+1,z)}(n-2)$$
$$=\frac{\prod_{l=2m}^{n-2}(q^j-1)}{2\prod_{j=1}^{n-2m-1}(q^j-1)}\prod_{j=0}^{m-1}(q^{2j+1}-1)q^{m(m-1)}. \tag{5.72}$$

$$k_{(2(m-1),0)}(n-2)=\frac{\prod_{j=2m-1}^{n-2}(q^j-1)}{2\prod_{j=1}^{n-2m-1}(q^j-1)}(q^{m-1}+1)$$
$$\cdot\prod_{j=0}^{m-2}(q^{2j+1}-1)q^{(m-1)^2}. \tag{5.73}$$

因此, 从 (5.71), (5.72) 和 (5.73) 得

$$p^{(2,0)}_{(2m+1,1)(2m,0)}(n)=\frac{(q-1)q^2\prod_{j=2m}^{n-2}(q^j-1)\prod_{j=0}^{n-2m}(q^{2j+1}-1)}{4\prod_{j=1}^{n-2m-1}(q^j-1)}.$$
$$\cdot[(q^{2m-1}-1)q^{4m^3-7m^2+2}+(q^{m-1}+1)] \tag{5.74}$$

因为

$$k_{(2,0)}(n)=\frac{(q^n-1)(q^{n-1}-1)q}{2(q-1)}, \tag{5.75}$$

$$k_{(2m,0)}(n)=\frac{\prod_{j=2m+1}^{n}(q^j-1)}{2\prod_{j=1}^{n-2m}(q^j-1)}(q^j+1)\prod_{j=0}^{m-1}(q^{2j+1}-1)q^{m^2}, \tag{5.76}$$

所以由命题 1.1(vi), (5.74), (5.75) 和 (5.76), 有

$$p^{(2m,0)}_{(2,0)(2m+1,1)}(n)=k_{(2,0)}(n)p^{(2,0)}_{(2m+1,1)(2m,0)}(n)/k_{(2m,0)}(n)$$
$$=\frac{(q^{2m-1}-1)(q^{n-2m}-1)(q^m+q^{m-1}+1)q^{2m}}{4(q^m+1)}.$$

如果取

$$\mathcal{M}=\{S\in S(n,q)|S\sim[S_{2m+1,z},0^{(n-2m-1)}]\},$$

再按前面的推导过程进行, 可得

$$p^{(2m,0)}_{(2,0)(2m+1,z)}(n)=\frac{(q^{2m}-1)(q^{n-2m}-1)(q^m+q^{m-1}+1)q^{2m}}{4(q^m+1)}.$$

(II) $p^{(2m,0)}_{(2,2)(2m+1,1)}(n)$ 和 $p^{(2m,0)}_{(2,2)(2m+1,z)}(n)$ 的计算.

设

$$S_1 = 0,\ S_2 = [1,\ -z,\ 0^{(m-2)}]$$

和 (5.62) 成立, 并且

$$S - S_2 \sim [S_{2m,\varnothing}, 0^{(n-2m)}]. \tag{5.64$'$}$$

令 $S \in \mathcal{M}$, 我们仍按 (5.29) 到 (5.33) 的步骤进行, 把 S 变成 (5.62). 再记 $\mathcal{M}(2t+\gamma, \Gamma)$ 是 $\mathcal{M}$ 中形如 (5.62) 的所有矩阵组成的集合, 那么 (5.63) 成立. 我们仍对 $M(2t+\gamma, \Gamma)$ 中 γ, Γ 的各种情形进行考察. 如同对 (I) 中 $p^{(2m,0)}_{(2,0)(2m+1,1)}(n)$ 的计算, 在以下情形 "$\gamma = 0,\ V = 0$", "$\gamma = 1,\ \Gamma = 1, \operatorname{rank} V = 1$","$\gamma = 1,\ \Gamma = 1, \operatorname{rank} V = 2$", "$\gamma = 2,\ V = 0$" 和 "$\gamma = 2, \operatorname{rank} V = 1$",(5.64) 不成立, 而以下情形: "$\gamma = 0, \operatorname{rank} V = 2$", "$\gamma = 1,\ \Gamma = z, \operatorname{rank} V = 1$"; "$\gamma = 1,\ \Gamma = z, \operatorname{rank} V = 2$"; 和 "$\gamma = 2, \operatorname{rank} V = 2$" 不出现. 所以只考虑 "$\gamma = 0, \operatorname{rank} V = 1$"; "$\gamma = 1, \Gamma = 1,\ V = 0$"; 和 "$\gamma = 1,\ \Gamma = z,\ V = 0$" 的情形.

(1) $\gamma = 0, \operatorname{rank} V = 1$. 这时 $t = m-1$, 按照 (I.i.b) 的推导, 可取 ${}^tV = \begin{pmatrix} \lambda & 0 & \cdots & 0 \\ \mu & 0 & \cdots & 0 \end{pmatrix}$ λ, μ 全不为 0, 当 $\mu \neq 0$ 时,(5.62) 可变成

$$\begin{pmatrix} U & 0 & \begin{pmatrix} \lambda & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \end{pmatrix} \\ 0 & M(2(m-1), \varnothing) & 0 \\ \begin{pmatrix} \lambda & 1 \\ 0 & 0 \\ \vdots & \vdots \\ 0 & 0 \end{pmatrix} & 0 & 0 \end{pmatrix},$$

从而有

$$\begin{vmatrix} a & b & \lambda \\ b & c & 1 \\ \lambda & 1 & 0 \end{vmatrix} = 2b\lambda - c\lambda^2 - a.$$

令 $c^* = 2b\lambda - c\lambda^2 - a$, 那么

$$\begin{vmatrix} a-1 & b & \lambda \\ b & c+z & 1 \\ \lambda & 1 & 0 \end{vmatrix} = c^* - z\lambda^2 + 1.$$

由 $S \sim [S_{2m+1,1},\ 0^{(n-2m-1)}]$, 有 $c^* \sim 1$, 当 $c^* = 2\lambda^2 - 1$ 时,(5.64)$'$ 式成立, 当 $c^* \neq 2\lambda^2 - 1$ 时,(5.64)$'$ 不成立; 当 $\lambda = 0,\ a = 1$ 时,(5.64)$'$ 也不成立. 所以 $\mathcal{M}(2(m-1), \varnothing)$ 中满足 (5.64)$'$ 的 S 的个数是

$$\left[\frac{1}{2}(q-1)(q^{n-2m}-1) + (q^{n-2m}-1)\right]q^2 = \frac{1}{2}(q+1)(q^{n-2m}-1)q^2. \tag{5.77}$$

(2) $\gamma = 1,\ \Gamma = 1,\ V = 0$. 这时 $t = m$ 或 $m-1$. 当 $t = m$ 时,$U = 0$, 显然 (5.64)

不成立. 当 $t=m-1$ 时 $U\sim\begin{pmatrix}0&1\\1&0\end{pmatrix}$. 如果

$$U-[1,\ -z]\sim[-1,\ 0], \tag{5.78}$$

则 (5.64)′ 成立, 否则 (5.64)′ 不成立, 而满足 (5.78) 的 U 的个数是

$$p^{(2,2)}_{(2,0)(1,0)}(2)=\frac{1}{4}(q^2-1), \tag{5.79}$$

即 $\mathcal{M}(2(m-1)+1,\ 1)$ 中满足 (5.64)′ 的 S 的个数是 $\frac{1}{4}(q^2-1)$.

(3) $\gamma=1, \Gamma=z, V=0$. 这时 $t=m-1, U\sim[1,\ -z]$, 如果

$$U-[1,\ -z]\sim(-z\quad 0), \tag{5.80}$$

则 (5.64)′ 成立, 否则 (5.64)′ 不成立, 而满足 (5.80) 的 U 的个数是

$$p^{(2,2)}_{(2,2)(1,z)}(2)=\frac{1}{4}(q^2-2q-3), \tag{5.81}$$

即 $\mathcal{M}(2(m-1)+1,\ z)$ 中满足 (5.64)′ 的 S 的个数是 $\frac{1}{4}(q^2-2q-3)$.

因此, 由 (5.63),(5.78),(5.80) 和 (5.82), 可得

$$\begin{aligned}p^{(2,2)}_{(2im+1,\,1)(2m,\,0)}(n)=&k_{(2(m-1)+1,\,1)}(n-2)q^{4m-2}\cdot\frac{1}{4}(q^2-1)\\&+k_{(2(m-1)+1,\,z)}(n-2)q^{4m-2}\cdot\frac{1}{4}(q^2-2q-3)\\&+k_{(2(m-1),\,\varnothing)}(n-2)q^{4m-4}\cdot\frac{1}{2}(q+1)(q^{n-2m}-1)q^2.\end{aligned} \tag{5.82}$$

由 (5.72), 有

$$k_{(2,2)}(n)=\frac{(q^n-1)(q^{n-1}-1)q}{2(q+1)}, \tag{5.83}$$

所以由命题 1.1 (iv), (5.77), (5.82) 和 (5.83), 可得

$$\begin{aligned}p^{(2m,0)}_{(2,2)(2m+1,\,1)}(n)&=k_{(2,2)}(n)\,p^{(2,2)}_{(2m+1,\,1)(2m,\,0)}(n)/k_{(2m,\,0)}(n)\\&=\frac{(q^{2m-1}-1)(q^{n-2m}-1)(q^m-q^{m-1}+1)q^{2m}}{4(q^m+1)}.\end{aligned}$$

同理

$$p^{(2m,0)}_{(2,2)(2m+1,\,z)}(n)=\frac{(q^{2m-1}-1)(q^{n-2m}-1)(q^m-q^{m-1}+1)q^{2m}}{4(q^m+1)}.$$

(III) $p^{(2m,2)}_{(2,0)(2m+1,\,1)}(n)$, $p^{(2m,2)}_{(2,0)(2m+1,\,z)}(n)$, $p^{(2m,2)}_{(2,2)(2m+1,\,1)}(n)$ 和 $p^{(2m,2)}_{(2,2)(2m+1,\,z)}(n)$ 的计算.

平行于 (I) 和 (II) 相应的推导, 可得

$$
\begin{aligned}
p^{(2m,\,2)}_{(2,\,0)(2m+1,\,1)}(n) =& p^{(2m,\,2)}_{(2,\,0)(2m+1,\,z)}(n)\\
=& \frac{(q^{2m}-1)(q^{n-2m}-1)(q^m+q^{m-1}-1)q^{2m}}{4(q^m-1)}.
\end{aligned}
$$

$$
\begin{aligned}
p^{(2m,\,2)}_{(2,\,2)(2m+1,\,1)}(n) =& p^{(2m,\,2)}_{(2,\,2)(2m+1,\,z)}(n)\\
=& \frac{(q^{2m-1}-1)(q^{n-2m}-1)(q^m-q^{m-1}-1)q^{2m}}{4(q^m-1)}.
\end{aligned}
$$

(IV) N_2 的计算.

当 $k=2m,\ \xi=0$, 而 $h=2m+1$ 时,

$$
\begin{aligned}
N_2 =& p^{(2m,\,0)}_{(2,\,0)(2m+1,\,1)}(n)+p^{(2m,\,0)}_{(2,\,0)(2m+1,\,z)}(n)\\
&+p^{(2m,\,0)}_{(2,\,2)(2m+1,\,1)}(n)+p^{(2m,\,0)}_{(2,\,2)(2m+1,\,z)}(n)\\
=& (q^{2m}-1)(q^{n-2m}-1)q^{2m}.
\end{aligned}
$$

当 $k=2m,\ \xi=2$, 而 $h=2m+1$ 时,

$$
\begin{aligned}
N_2 =& p^{(2m,\,2)}_{(2,\,0)(2m+1,\,1)}(n)+p^{(2m,\,2)}_{(2,\,0)(2m+1,\,z)}(n)\\
&+p^{(2m,\,2)}_{(2,\,2)(2m+1,\,1)}(n)+p^{(2m,\,2)}_{(2,\,2)(2m+1,\,z)}(n)\\
=& (q^{2m}-1)(q^{n-2m}-1)q^{2m}.
\end{aligned}
$$

□

设 Γ 是以 X_n 为顶点集, 以 $\overline{R}_1$ 为边集的图, 显然这个图是无向的. 再由定理 5.5 可知这个图是连通的, 易见 $\overline{R_i}$ 为图 Γ 中距离为 i 的点对之集合. 于是由引理 5.14 和定理 1.24, 立即得到

定理 5.15　如果在 X_n 上定义了结合关系 $\overline{R}_i\,(i=0,\,1,\cdots,\,[\frac{n+1}{2}])$, 那么 $\mathcal{X}=(X_n,\,\{\overline{R}_i\}_{0\leqslant i\leqslant[\frac{n+1}{2}]})$ 是一个对称结合方案, 记作 Quad$\,(n,\,q)$. 进一步,Quad$\,(n,\,q)$ 与 Alt$\,(n+1,\,q)$ 有相同的参数, 因而是自对偶的, 并且是 (P 和 Q) 多项式的.

注: 文献中 Quad$\,(n,\,q)$ 也表示这个结合方案的第一个结合关系 $\overline{R}_1$ 的图.

定理 5.16　设 $n\geqslant 3$, 那么结合方案 Quad$(n,\,q)$ 的第一个结合关系 $\overline{R}_1$ 的图 Γ 不是距离可迁的, 因而它不与结合方案 Alt$(n+1,q)$ 同构.

证明　为了证明本定理需要引入一个符号. 设 $\mathcal{M}$ 为 X_n 的一个非空子集, 令

$$\mathcal{M}^{\perp}=\{X\in X_n|\mathrm{rank}(X-S)\leqslant 2,\ \forall S\in\mathcal{M}\}.$$

特别是, 对于图 Γ 的两个邻接点 S_1 和 S_2, $\{S_1,\,S_2\}^{\perp\perp}$ 叫做 Γ 的一条奇异直线 (singular line). 下面我们分两种情况讨论两对邻接点确定的奇异直线.

(a) 设 $S_1=0,\ S_2=E_{11}$, 往证 $\{0,\,E_{11}\}^{\perp\perp}=\{aE_{11}|a\in\mathbb{F}_q\}$.

首先注意到,0, $\lambda_1 E_{11}+\lambda_2 E_{22}\in\{0,\ E_{11}\}^{\perp}$. 设对称矩阵 $S\in\{0,\ E_{11}\}^{\perp\perp}$, 那么 $\operatorname{rank} S\leqslant 2$. 记

$$S=\begin{pmatrix} s_{11} & s_{12} & \cdots & s_{1n}\\ s_{12} & s_{22} & \cdots & s_{2n}\\ \vdots & \vdots & & \vdots\\ s_{1n} & s_{2n} & \cdots & s_{nn}\end{pmatrix},$$

那么对于任意的 $\lambda_1,\ \lambda_2\in\mathbb{F}_q$, 有

$$\operatorname{rank}\begin{pmatrix} s_{11}-\lambda_1 & s_{12} & \cdots & s_{1n}\\ s_{12} & s_{22}-\lambda_2 & \cdots & s_{2n}\\ \vdots & \vdots & & \vdots\\ s_{1n} & s_{2n} & \cdots & s_{nn}\end{pmatrix}\leqslant 2.$$

于是对于 $3\leqslant j,\ k\leqslant n$, 恒有

$$\begin{vmatrix} s_{11}-\lambda_1 & s_{12} & s_{1k}\\ s_{12} & s_{22}-\lambda_2 & s_{2k}\\ s_{1j} & s_{2j} & s_{jk}\end{vmatrix}=0.$$

令 $\lambda_1=0$ 和 1 分别代人上式, 然后将所得两式相减, 就得到

$$\begin{vmatrix} s_{22}-\lambda_2 & s_{2k}\\ s_{2j} & s_{jk}\end{vmatrix}=0.$$

再将 $\lambda_2=0$ 和 1 分别代人上式, 就得到

$$s_{jk}=0,\ \ 3\leqslant j,\ k\leqslant n.$$

取 $j=k$ 我们可得到

$$s_{2k}=0,\ 3\leqslant k\leqslant n.$$

同样的办法, 我们可得

$$s_{1k}=0,\ 3\leqslant k\leqslant n.$$

所以

$$S=\left[\begin{pmatrix} s_{11} & s_{12}\\ s_{12} & s_{22}\end{pmatrix},\ 0^{(n-2)}\right].$$

再由 $E_{13}+E_{31}\in\{0,\ E_{11}\}^{\perp}$, 可推出 $s_{22}=0$, 由 $E_{11}+E_{22}\in\{0,\ E_{11}\}^{\perp}$ 推出 $s_{12}=0$, 即 $S=s_{11}E_{11}$. 令 $\mathcal{N}=\{aE_{11}\}$. 我们证明了 $\{0,\ E_{11}\}^{\perp\perp}\subseteq\mathcal{N}$.

下面我们要证明 $\mathcal{N} \subseteq \{0, E_{11}\}^{\perp\perp}$. 只要证明 $\{0, E_{11}\}^{\perp} \subseteq \mathcal{N}^{\perp}$. 设 $T \in \{0, E_{11}\}^{\perp}$. 那么 $\operatorname{rank} T \leqslant 2$. 如果 $T = 0$, 显然 $T \in \mathcal{N}^{\perp}$. 设 $T \neq 0$. 写

$$T = \begin{pmatrix} t_{11} & {}^tT_{12} \\ T_{12} & T_{22} \end{pmatrix} \begin{matrix} 1 \\ n-1 \end{matrix}.$$

如果 $T_{22} = 0$, 那么显然有 $T \in \mathcal{N}^{\perp}$. 如果 $\operatorname{rank} T_{22} = 1$, 那么存在 $P \in GL_{n-1}(\mathbb{F}_q)$ 使得 $PT_{22}{}^tP = [1, 0]$, 于是

$$[1, P]\begin{pmatrix} t_{11} & {}^tT_{12} \\ T_{12} & T_{22} \end{pmatrix}{}^t[1, P] = \begin{pmatrix} t_{11} & t_{12} & {}^tT_{13} \\ t_{12} & 1 & 0 \\ T_{13} & 0 & 0 \end{pmatrix}.$$

因为 $\operatorname{rank} T \leqslant 2$, 必有 $T_{13} = 0$, 由此我们可得 $T \in \mathcal{N}^{\perp}$. 如果 $\operatorname{rank} T = 2$, 那么存在 $P \in GL_{n-1}(\mathbb{F}_q)$ 使得 $PT_{22}{}^tP = [A, 0]$, 这里 $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ 或 $[-1, z]$,

$$[1, P]T\,{}^t[1, P] = \begin{pmatrix} t_{11} & {}^tT_{12}^* & {}^tT_{13}^* \\ T_{12}^* & A & 0 \\ T_{13}^* & 0 & 0 \end{pmatrix}.$$

对上式再施行由 $\left[\begin{pmatrix} 1 & -{}^tT_{12}^*A^{-1} \\ & I \end{pmatrix}, I\right]$ 所引起的合同变换, 那么右端变成

$$\begin{pmatrix} t_{11}^* & 0 & {}^tT_{13}^* \\ 0 & A & 0 \\ T_{13}^* & 0 & 0 \end{pmatrix}.$$

由 $\operatorname{rank} T \leqslant 2$ 推出 $T_{13}^* = 0, t_{11}^* = 0$. 但 $[0, A, 0] \notin \{0, E_{11}\}^{\perp}$, 所以 $\operatorname{rank} T_{22} = 2$ 这种情形不会发生. 这样, 我们就证明了 $\{0, E_{11}\}^{\perp} \subseteq \mathcal{N}^{\perp}$. 由此立得 $\{0, E_{11}\}^{\perp\perp} \supseteq \mathcal{N}^{\perp\perp}$. 前面已经证明了 $\{0, E_{11}\}^{\perp\perp} \subseteq \mathcal{N}$. 而 $\mathcal{N} \subseteq \mathcal{N}^{\perp\perp}$, 所以 $\{0, E_{11}\}^{\perp\perp} = \mathcal{N}$.

(b) 设 $S_1 = 0, S_2 = E_{12} + E_{21}$ 或 $-E_{11} + zE_{22}$, 往证 $\{0, S_2\}^{\perp\perp} = \{0, S_2\}$.

设 $S_2 = E_{12} + E_{21}$, 并设 $S \in \{0, E_{12} + E_{21}\}^{\perp\perp}$. 注意到 $\lambda_1 E_{11} + \lambda_2 E_{22} \in \{0, E_{12} + E_{21}\}^{\perp}$ 对任意 $\lambda_1, \lambda_2 \in \mathbb{F}_q$. 由 (a) 中的证明可知 S 具有如下形状

$$S = \left[\begin{pmatrix} s_{11} & s_{12} \\ s_{12} & s_{22} \end{pmatrix}, 0^{(n-2)}\right].$$

令

$$\begin{vmatrix} 0 & -1 & x \\ -1 & 0 & y \\ x & y & \omega \end{vmatrix} = -2xy - \omega = 0, \text{即 } \omega = -2xy,$$

那么, 对于任意 $x, y \in \mathbb{F}_q$, $x(E_{13}+E_{31})+y(E_{23}+E_{32})-2xyE_{33} \in \{0, E_{12}+E_{21}\}^{\perp}$, 我们有

$$\begin{vmatrix} -s_{11} & -s_{12} & x \\ -s_{12} & -s_{22} & y \\ x & y & -2xy \end{vmatrix} = -2(s_{11}s_{22}+s_{12}-s_{12}^2)xy+s_{22}x^2+s_{11}y^2=0,$$

对任意 $x, y \in \mathbb{F}_q$, 这就推出 $s_{11}=s_{22}=0$, $s_{12}-s_{12}^2=0$. 如果 $s_{12}=0$, 那么 $S=0$. 如果 $s_{12}\neq 0$, 那么 $s_{12}=1$, 即 $S=E_{12}+E_{21}$. 于是 $\{0, E_{12}+E_{21}\}^{\perp\perp}=\{0, E_{12}+E_{21}\}$.

同样的方法可证 $\{0, -E_{11}+zE_{22}\}^{\perp\perp}=\{0, -E_{11}+zE_{22}\}$.

现在, 假设图 Γ 是距离可迁的, 由于 $\{0, E_{11}\}$ 和 $\{0, E_{12}+E_{21}\}$ 是两对邻接点, 就应有 Γ 的自同构 σ 使 $\{0, E_{11}\}^{\sigma}=\{0, E_{12}+E_{21}\}$, 从而有 $(\{0, E_{11}\}^{\perp\perp})^{\sigma}=\{0, E_{12}+E_{21}\}^{\perp\perp}$. 但 $|\{0, E_{11}\}^{\perp\perp}|=q$, 而 $|\{0, E_{12}+E_{21}\}|=2$, 这就导致矛盾. □

§5.8 对称矩阵结合方案的自对偶性

我们已知 $\mathbb{F}_q$ 上全体 $n\times n$ 对称矩阵对于矩阵的加法作成一个加法群. 在这一节中要证明对称矩阵结合方案 $\mathrm{Sym}(n, q)$ 是自对偶的.

令 χ 是基域 $\mathbb{F}_q$ 的加法群 $(\mathbb{F}_q, +)$ 的一个非平凡的特征标. 对于每个对称矩阵 $A=(a_{ij})\in S(n, q)(a_{ij}=a_{ji})$, 我们定义一个映射

$$\begin{aligned} \phi_A: S(n, q) &\longrightarrow \mathbb{C} \\ X=(x_{ij}) &\longmapsto \chi(\textstyle\sum_{i=1}^n\sum_{j=1}^n a_{ij}x_{ij})\ (x_{ij}=x_{ji}), \end{aligned}$$

那么 ϕ_A 是 $S(n, q)$ 的一个不可约特征标. 并且有

$$\phi_{A+B}=\phi_A\phi_B.$$

定理 5.17 设 $A, B\in S(n, q)$, 那么 $\phi_A=\phi_B$ 当且仅当 $A=B$. 于是 $A\longrightarrow\phi_A$ 是 $S(n, q)$ 到它特征标群 $S(n, q)^*$ 的一个同构.

证明 先证定理的前一个论断, 充分性是显然的. 下面证明必要性. 设 $\phi_A=\phi_B$, 而 $A=(a_{ij})$ 和 $B=(b_{ij})$ 都属于 $S(n, q)$. 那么

$$\chi\Big(\sum_{i=1}^n\sum_{j=1}^n a_{ij}x_{ij}\Big)=\chi\Big(\sum_{i=1}^n\sum_{j=1}^n b_{ij}x_{ij}\Big),\ \forall x_{ij}\in\mathbb{F}_q.$$

对于 i, j, 当 $i=j$ 时, 取 $x_{kl}=0$, $k\neq i$, $l\neq i$. 那么

$$\chi(a_{ii}x_{ii})=\chi(b_{ii}x_{ii}),\ \forall x_{ii}\in\mathbb{F}_q.$$

即

$$\chi((a_{ii}-b_{ii})x_{ii})=1,\ \forall x_{ii}\in \mathbb{F}_q.$$

因 $\chi\neq 1$ (因 χ 是非平凡的特征标), 所以 $a_{ii}=b_{ii}\,(i=1,2,\cdots,n)$.

当 $i>j$ 时, 取 $x_{kl}=0,\ k\neq i,\ l\neq j$. 那么

$$\chi(2a_{ij}x_{ij})=\chi(2b_{ij}x_{ij}),\ \forall x_{ij}=x_{ji}\in \mathbb{F}_q.$$

再由 $\chi\neq 1$, 有 $a_{ij}=b_{ij}\,(i>j)$, 因此 $A=B$.

定理的后一论断是明显的. □

定理 5.18　对于 $A,\ X\in S(n,q)$ 及 $T\in GL_n(\mathbb{F}_q)$, 恒有

$$\phi_A(TX\,{}^tT)=\phi_{{}^tTAT}(X). \tag{5.84}$$

证明　设 $A=(a_{ij}),\ a_{ij}=a_{ji},\ X=(x_{ij}),\ x_{ij}=x_{ji},\ T=(t_{ij})$, 再令 $TX\,{}^tT=(x^*_{ij}),\ {}^tTAT=(a^*_{ij})$, 那么 $x^*_{ij}=\sum_{k=1}^n\sum_{l=1}^n t_{ik}x_{kl}t_{jl},\ a^*_{ij}=\sum_{k=1}^n\sum_{l=1}^n t_{ki}a_{kl}t_{lj}$. 注意到 A, X 是对称矩阵, 易见有

$$\sum_{i=1}^n\sum_{j=1}^n a_{ij}x^*_{ij}=\sum_{i=1}^n\sum_{j=1}^n a^*_{ij}x_{ij},$$

所以 (5.85) 成立.

令 $\mathbb{C}_{(i,\xi)}$ 表示合同类 $C_{(i,\xi)}$ 在 $S(n,q)$ 的群代数 $\mathbb{C}S(n,q)$ 中的形式和,$\mathfrak{S}$ 为由 $\mathbb{C}_0=\mathbb{C}_{(0,0)},\mathbb{C}_{(1,\xi)},\cdots,\mathbb{C}_{(n,\xi)}(\xi=1,z)$ 生成的 S 环, 由 $\mathfrak{S}$ 确定的结合方案 $\mathfrak{X}(\mathfrak{S})$ 就是 $\mathrm{Sym}(n,q)$. 令

$$\phi_A(\mathbb{C}_{(i,\xi)})=\sum_{X\in\mathbb{C}(i,\xi)}\phi_A(X),\ i=0,1,\cdots,n,\xi=1\text{ 或 }z,$$

那么 $\phi_A(\mathbb{C}_{(i,\xi)})$ 是 $\mathrm{Sym}(n,q)$ 的邻接矩阵 $A_{(i,\xi)}$ 的特征值, 属于特征向量 ϕ_A. 由定理 5.17 知, 对于 $A,\ B\in S(n,q)$, 如果

$$\phi_A(\mathbb{C}_{(i,\xi)})=\phi_B(\mathbb{C}_{(i,\xi)}),\ i=0,1,\cdots,n,\ \xi=1\text{ 或 }z,$$

那么 A 和 B 在同一等价类中. 于是由定理 1.14 在 $S(n,q)^*$ 上确定的等价类 $Y_{(j,\xi)}$ 恰为

$$Y_{(j,\xi)}=\{\phi_A|A\in\mathbb{C}_{(j,\xi)}\},\ j=0,1,\cdots,n,\ \xi=1\text{ 或 }z.$$

相应地得到 $S(n,q)^*$ 上的一个 S 环 $\mathfrak{S}^*$. 由 $\mathfrak{S}^*$ 确定的结合方案 $\mathfrak{X}(\mathfrak{S})^*$ 和 $\mathrm{Sym}(n,q)$ 是形式对偶的.

现在映射 $A\longrightarrow\phi_A$ 是 $S(n,q)$ 到 $S(n,q)^*$ 的一个同构对应, 它诱导出结合方案 $\mathrm{Sym}(n,q)$ 和 $\mathfrak{X}(\mathfrak{S}^*)$ 的一个同构. 因此, 我们得到

定理 5.19　对称矩阵结合方案 $\mathrm{Sym}(n,q)$ 是自对偶的.

§5.9 对称矩阵结合方案的自同构

关于对称矩阵结合方案 Sym(n,q) 的自同构, 我们有下面的

定理 5.20 设 $n \geqslant 2$, Sym(n,q) 为 $\mathbb{F}_q$ 上 n 阶对称矩阵的结合方案.

(i) Sym(n,q) 的每个自同构 f 具有如下的形状

$$f: X \longrightarrow \xi P X^{\sigma}\, {}^tP + S_0, \forall\, X \in S(n,q), \tag{5.85}$$

这里 $\xi = 1$ 或 z(z 为 $\mathbb{F}_q$ 中取定的一个非平方元), $P \in GL_n(\mathbb{F}_q)$, $S_0 \in S(n,q)$, σ 为 $\mathbb{F}_q$ 的自同构.

(ii) Aut Sym(n, q): Inn Sym$(n, q) = 2$.

证明 容易看出, 形如 (5.85) 的映射 f 是 Sym(n, q) 的一个自同构, 特别是 $f_z : X \to zX$ 使得

$$f_z R_{(i,\xi)} = \begin{cases} R_{(i,\xi)}, & \text{如果}\, i\, \text{为偶数}, \\ R_{(i,\xi')}, & \text{如果}\, i\, \text{为奇数}, \end{cases}$$

这里 $1' = z$, $z' = 1$.

设 $q = p^t$, p 为奇素数. 由定理 5.10, 结合方案 Sym(n, q) 的价 $k_{(i,\xi)}(n)$ 所含 p 的幂为 p^{ts^2}(当 $i = 2s$ 时) 或 $p^{ts(s+1)}$(当 $i = 2s+1$), 因此, 当 $i \neq j$ 时,$k_{(i,*)}(n) \neq k_{(j,*)}(n)$.

现在, 设 f 是 Sym(n, q) 的一个自同构, 于是可知 $fR_{(i,*)} = R_{(i,*)}$, 特别是 $fR_{(1,*)} = fR_{(1,*)}$. 这就是说, 对于 $X, Y \in S(n, q)$, 如果 rank$(X - Y) = 1$, 那么 rank$(f(X) - f(Y)) = 1$. 当 $n \geqslant 2$ 时, 由对称矩阵几何基本定理 ([16] Theorem 5.4) 可知 f 具有形状 (5.85).

(ii) 中论断是显然的. □

关于结合方案 Quad(n, q) 的自同构我们有如下

定理 5.21 设 $n \geqslant 3$. 结合方案 Quad(n, q) 的自同构都是内自同构并且具有形状 (5.85).

证明 Quad(n, q) 的结合类 $\overline{R}_i$ 的价为

$$\overline{k}_i(n) = \textstyle\sum_{\xi=1,z}(k_{(2i-1,\xi)}(n) + k_{(2i,\xi)}(n))$$

$$= q^{(i-1)i}\frac{\prod\limits_{j=i+1}^{n+1}(q^i - 1)}{\prod\limits_{j=1}^{n-2i+1}(q^i-1)\cdot\prod\limits_{j=1}^{i}(q^i+1)}.$$

由此可知, 这些 $\overline{k}_i(n)(i = 1, 2, \cdots, [\frac{n+1}{2}])$ 两两不等, 于是 Quad(n, q) 的任一自同构 $\mathcal{A}$ 是每个关系图 $\overline{G}_i$ 的自同构, 因而是内自同构. 特别是 $\mathcal{A} \in \mathrm{Aut}\overline{\Gamma}_1$, 即对于任二对称矩阵 X, Y 都有 rank$(Y - X) \leqslant 2$ 当且仅当 rank$(\mathcal{A}(Y) - \mathcal{A}(X)) \leqslant 2$.

进一步, 如果 $\mathrm{rank}(Y-X)=1$, 那么由定理 5.16 的证明可知 $|\{X, Y\}^{\perp\perp}|=q$, 从而 $|\{\mathcal{A}(X), \mathcal{A}(Y)\}^{\perp\perp}|=q$, 于是 $\mathrm{rank}(\mathcal{A}(Y)-\mathcal{A}(X))=1$. 由定理 5.20 立得 $\mathcal{A}$ 具有形状 (5.85). □

最后, 我们来看 $n=1$ 时 $\mathrm{Sym}\,(1, n)$ 的自同构如何?

当 $n=1$ 时, $\mathrm{Sym}\,(1, n)$ 的非平凡结合类只有两个: R_1, R_z, 这里

$$R_1=\{(x, y)|y-x\in \mathbb{F}_q^{*2}\}, \qquad R_2=\{(x, y)|y-x\in z\mathbb{F}_q^{*2}\}.$$

对应于 R_1 的图 $\Gamma^{(1)}$ 叫做 Paley 图. M. E. Muzichuk[13] 证明了下面的

定理 5.22 设 $q=p^n$, p 为奇素数.Paley 图的任一自同构 φ 具有如下形状

$$\varphi: x\longrightarrow ax^{p^i}+b,\ \forall x\in \mathbb{F}_q, \tag{5.86}$$

这里 $a\in \mathbb{F}_q^{*^2}$, $b\in \mathbb{F}_q$, $i=0, 1, \cdots, n-1$.

由于证明很初等, 我们在这里介绍. 设 φ 是 $\mathbb{F}_q$ 到 $\mathbb{F}_q$ 的任意一个映射 (或称函数). 对于自然数 $k(k\leqslant q)$, 记 $\sigma_k(\varphi)$ 是 $\varphi(\alpha)(\alpha\in \mathbb{F}_q)$ 的 k 次初等对称函数, 即

$$\sigma_k(\varphi)=\sum_{*}\varphi(\alpha_1)\cdots\varphi(\alpha_k),$$

这里 $*$ 遍及 $\mathbb{F}_q$ 的全体 k 子集 $\{\alpha_1, \cdots, \alpha_k\}$.

引理 5.23 设 $\varphi:\mathbb{F}_q\longrightarrow \mathbb{F}_q$. 那么下面条件等价:

(i) φ 是单的 (因而是 1–1 到上的);

(ii) $\prod_{\alpha\in \mathbb{F}_q}(z-\varphi(\alpha))=z^q-z$;

(iii) $\sigma_k(\varphi)=\begin{cases}0, & \text{如果 } 1\leqslant k\leqslant q \text{ 而 } k\neq q-1,\\ -1, & \text{如果 } k=q-1;\end{cases}$

(iv) $\sum_{\alpha\in \mathbb{F}_q}\varphi^k(\alpha)=\begin{cases}0, & \text{如果 } 0\leqslant k\leqslant q-2,\\ -1, & \text{如果 } k=q-1.\end{cases}$

(注意: 这里 $\varphi^0=1$ 为恒 1 映射.)

证明 (i) $\Longleftrightarrow$ (ii) $\Longleftrightarrow$ (iii) 是明显的. 记 σ_k 为不定元 $x_1, \cdots, x_q$ 的 k 次初等对称多项式,$s_k=\sum_{i=1}^q x_i^k$. 熟知有牛顿恒等式: $s_k-\sigma_1 s_{k-1}+\sigma_2 s_{k-2}-\cdots+(-1)^{k-1}\sigma_{k-1}s_1+(-1)^k k\sigma_k=0$, $1\leqslant k\leqslant q$. 由此可知 (iii) $\Longrightarrow$ (iv). 下面我们证明 (iv) $\Longrightarrow$ (i).

假设 φ 不是单的, 设 $\{y_1, \cdots, y_m\}$ 为 φ 的全体不同的函数值, 这里 $m<q$, 那么对所有 $\alpha\in \mathbb{F}_q$ 均有 $(\varphi(\alpha)-y_1)(\varphi(\alpha)-y_2)\cdots(\varphi(\alpha)-y_m)=0$. 于是 φ^m 可表示成 $\varphi^{m-1}, \cdots, \varphi, 1$ 的线性组合, 因而对于任意 l, φ^l 均可表示为 $\varphi^{m-1}, \cdots, \varphi, 1$ 的

线性组合. 特别是可设 $\varphi^{q-1}=\sum_{i=0}^{m-1}\beta_i\varphi^i$. 这样, 由 (iv) 就有

$$-1=\sum_{\alpha\in\mathbb{F}_q}\varphi^{q-1}(\alpha)=\sum_{i=0}^{m-1}\beta_i\sum_{\alpha\in\mathbb{F}_q}\varphi^i(\alpha)=0,$$

导致矛盾. □

对于任给映射 $\varphi:\mathbb{F}_q\longrightarrow\mathbb{F}_q$, 令 $A_\varphi=\{\frac{\varphi(\alpha)-\varphi(\beta)}{\alpha-\beta}|\alpha,\beta\in\mathbb{F}_q,\alpha\neq\beta\}$. 注意到, 当 φ 是图 $\Gamma^{(1)}$ 的自同构时,$A_\varphi\subseteq\mathbb{F}_q^{*^2}$, 因而 $|A_\varphi|\leqslant\frac{1}{2}(q-1)$.

引理 5.24 设 $\varphi:\mathbb{F}_q\longrightarrow\mathbb{F}_q$ 不是单映射, 并且 $|A_\varphi|\leqslant\frac{1}{2}(q-1)$. 那么, 对于任意整数 $k\geqslant0$ 均有

$$\sum_{\alpha\in\mathbb{F}_q}\varphi^k(\alpha)=0.$$

证明 实际上只需考虑 $1\leqslant k\leqslant q-1$. 对于任意 $a\in\mathbb{F}_q$, 令 $\varphi_a(x)=\varphi(x)-ax$, 再令 $P_k(a)=\sigma_k(\varphi_a)$. 那么,$P_k(a)$ 可表示成 a 的多项式, 当 $1\leqslant k\leqslant q-2$ 时, 其 a^k 的系数为 0. 因此,$P_k(a)$ 作为 a 的多项式其次数 $\leqslant k-1$. 又当 $a\in\mathbb{F}_q\backslash A_\varphi$ 时, φ_a 是单映射, 于是由引理 5.23(iii) 可知,$P_k(a)=\sigma_k(\varphi_a)=0$, 由于 $|\mathbb{F}_q\backslash A_\varphi|=q-|A_\varphi|\geqslant\frac{1}{2}(q-1)$, 所以, 当 $1\leqslant k\leqslant\frac{1}{2}(q+1)$ 时, 多项式 $P_k(a)\equiv0$. 因而 $\sigma_k(\varphi)=P_k(0)=0$. 这样, 我们有

$$\psi(z)=\prod_{\alpha\in\mathbb{F}_q}(z-\varphi(\alpha))=z^q+f(z),$$

这里

$$f(z)=a_{\frac{q-1}{2}}z^{\frac{q-1}{2}}+\cdots+a_1z+a_0.$$

现在, 设 $\{y_1,\cdots,y_m\}$ 是 φ 的全体不同函数值, 那么 $m<q$. $\psi(y_i)=0,i=1,\cdots,m$. 由于 $\mathbb{F}_q$ 的元素都是 z^q-z 的根, 所以 $\{y_1,\cdots,y_m\}$ 都是 $f(z)+z$ 的根.

因为 φ 不是单的, 由引理 5.23, $\psi(z)\neq z^q-z$, 所以 $f(z)+z$ 不是零多项式, 于是推出 $m\leqslant\frac{1}{2}(q-1)$.

设 n_i 为 y_i 的重数, 那么 y_i 为 ψ' 的 n_i-1 重根. 注意到 $\sum_{i=1}^m(n_i-1)=q-m\geqslant\frac{1}{2}(q+1)$, 而 $\psi'=f'$, 且 f' 的次 $\leqslant\frac{1}{2}(q-3)$, 所以 $\psi'=f'\equiv0$. 这样. 存在某个多项式 h 使得 $\psi=h^p$. 又因为 $\psi(z)=\prod_{i=1}^m(z-y_i)^{n_i}$, 所以 $n_i\equiv0(\bmod p)$. 于是对于任意 $n\geqslant0$ 均有

$$\sum_{\alpha\in\mathbb{F}_q}\psi^n(\alpha)=\sum_{i=1}^m n_iy_i^n=0.$$

□

现在, 我们证明定理 5.22. 显然, 形如 (5.86) 的映射都是 Paley 图 $\Gamma^{(1)}$ 的自同构. 设 φ 是 $\Gamma^{(1)}$ 的任一自同构, 往证 φ 具有形状 (5.86). 设 $\varphi(0)=b$, 使 φ 承受自

同构 $x \longmapsto x-b$ 后, 可设 $\varphi(0)=0$. 由于 φ 为有限域 $\mathbb{F}_q$ 到 $\mathbb{F}_q$ 的一个函数, 因此可设 φ 为 $\mathbb{F}_q$ 上的一个次数 $\leqslant q-1$ 的多项式. 再由 $\varphi(0)=0$, 可设

$$\varphi(x)=c_1x+c_2x^2+\cdots+c_{q-1}x^{q-1}, \forall x \in \mathbb{F}_q.$$

下面分三步证明:

(1) 我们证明: $\varphi(x)$ 的非 0 项的次数是 p 的幂, 即

$$\varphi(x)=a_0x+a_1x^p+a_2x^{p^2}+\cdots+a_{n-1}x^{p^{n-1}}.$$

设 φ 的某个项的次数 $i=p^m l$, 而 $(l, p)=1$ 且 $l \geqslant 2$. 往证 $c_i=0$. 令 $f=\varphi^{p^{n-m}}$, 于是 f 也是图 $\Gamma^{(1)}$ 的自同构且 $f(0)=0$. 又显然有 $|A_f| \leqslant \frac{1}{2}(q-1)$. 那么, 对于任意 $a \in \mathbb{F}_q$ 均有

$$\sum_{\alpha \in \mathbb{F}_q}(f(\alpha)-a\alpha)^k=0, \quad 1 \leqslant k \leqslant q-2.$$

这是因为当 $a \notin A_f$ 时,$f_a(x)=f(x)-ax$ 是单的, 由引理 5.23 知上式成立; 当 $a \in A_f$ 时,$f_a(x)=f(x)-ax$ 不是单的, 并且 $|A_{f_a}|=|A_f| \leqslant \frac{1}{2}(q-1)$. 由引理 5.24 知上式也成立.

将上式左边写成 a 的多项式就有 $\sum_{t=0}^{k}(-1)^t c_k^t(\sum_{\alpha \in \mathbb{F}_q} f^{k-t}(\alpha)\alpha^t)a^t=0$, 于是可知其系数均为 0, 特别考虑 a^{k-1} 的系数就得 $k\sum_{\alpha \in \mathbb{F}_q} f(\alpha)\alpha^{k-1}=0$.

现在, 我们取 $k=q-l \leqslant q-2$, 这时 $(k, p)=1$, 于是得 $\sum_{\alpha \in \mathbb{F}_q} f(\alpha)\alpha^{q-l-1}=0$. 对此取 p^m 次幂, 注意到 $f(\alpha)^{p^m}=\varphi(\alpha)^{p^n}=\varphi(\alpha)$, $\alpha^{(q-l-1)p^m}=\alpha^{-i}$, 于是有 $\sum_{\alpha \in \mathbb{F}_q}\varphi(\alpha)\alpha^{-i}=0$. 将 $\varphi(\alpha)=\sum_{j=1}^{q-1}c_j\alpha^j$ 代入, 有 $\sum_{j=1}^{q-1}c_j\sum_{\alpha \in \mathbb{F}_q}\alpha^{j-i}=0$. 由引理 5.23 可知 $c_i=0$.

(2) 令 t 为$\mathbb{F}_q$ 到 $\mathbb{F}_q$ 的如下映射: $t(0)=0, t(x)=\frac{1}{x}, \forall \in \mathbb{F}_{q^*}$. 我们断言: $\psi=t\varphi t$ 为图 $\Gamma^{(1)}$ 的自同构且 $\psi(0)=0$.

$\psi(0)=0$ 是显然的. 设 (α, β) 是 $\Gamma^{(1)}$ 的任意一个边, 往证 $(\psi(\alpha), \psi(\beta))$ 也是 $\Gamma^{(1)}$ 的一个边. 就是说, 如果 $\beta-\alpha \in \mathbb{F}_q^{*^2}$, 那么有 $\psi(\beta)-\psi(\alpha) \in \mathbb{F}_q^{*^2}$.

先设 $\alpha\beta=0$, 不妨设 $\beta=0$. 这时 $-\alpha \in \mathbb{F}_q^{*^2}$. 由于 $-\psi(\alpha)=-t(\varphi(t(\alpha)))=-1/\varphi(1/\alpha)=1/\varphi(1/(-\alpha))$(注意到 φ 的非 0 项的次数为 p 的幂), 并且 φ 将平方元映到平方元, 所以 $-\varphi(\alpha) \in \mathbb{F}_q^{*^2}$.

现在设 $\alpha\beta \neq 0$. 由于

$$\frac{\psi(\beta)-\psi(\alpha)}{\beta-\alpha}=\frac{\psi(1/\alpha)-\psi(1/\beta)}{1/\alpha-1/\beta} \cdot \frac{1/\alpha}{\psi(1/\alpha)} \cdot \frac{1/\beta}{\psi(1/\beta)},$$

而右端三个乘积因子均为平方元, 所以其乘积为平方元, 于是 ψ 为 $\Gamma^{(1)}$ 的自同构.

(3) 由 (1) 和 (2), 可设 $\psi(x) = b_0x + b_1x^p + \cdots + b_{n-1}x^{p^{n-1}}$. 对于 $x \neq 0$ 恒有 $\psi(1/x)\psi(x) = 1$, 即

$$(a_0x^{-1} + a_1x^{-p} + \cdots + a_{n-1}x^{-p^{n-1}})(b_0x + b_1x^p + \cdots + b_{n-1}x^{p^{n-1}}) = 1.$$

两边乘以 $x^{p^{n-1}}$, 有

$$(a_0x^{p^{n-1}-1} + a_1x^{p^{n-1}-p} + \cdots + a_{n-1})(b_0x + b_1x^p + \cdots + b_{n-1}x^{p^{n-1}}) = x^{p^{n-1}}.$$

左边乘积中 x 的次数最高为 $2(p^{n-1} - 1) < q - 1$, 而上式被每个 $x \in \mathbb{F}_q^*$ 所满足. 因此上式为恒等式, 于是只有一个 $a_i \neq 0$, 其余 $a_j = 0$, 即 $\psi(x) = a_ix^{p^i}$. 又 $\psi(1) = a_i$ 所以 a_i 为平方元. 于是定理 5.22 得证. □

由定理 5.22 立刻可得下面

定理 5.25 Sym(1, q) 的自同构 $\mathcal{A}$ 具有形状

$$\mathcal{A}(x) = ax^{\sigma} + b, \ \ \forall x \in \mathbb{F}_q, \tag{5.87}$$

这里 $a \in \mathbb{F}_q^*$, $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$, $b \in \mathbb{F}_q$.

证明 因为 Sym(1, q) 的非平凡结合类只有两个: R_1 和 R_z, 如果 $\mathcal{A} : R_1 \to R_z$, 那么使 $\mathcal{A}$ 承受一个自同构 $\phi : x \longrightarrow zx$, $\forall x \in \mathbb{F}_q$, $\phi\mathcal{A}$ 就使 R_1 不变. 由定理 5.22, $\phi\mathcal{A}$ 具有形状 (5.86). 因而 $\mathcal{A}$ 有形状 (5.87). □

第六章　偶特征数的对称矩阵结合方案

§6.1　对称矩阵的标准形式及结合方案的构作

在这一章中, 恒设 q 为 2 的幂. 这时, q 元有限域 $\mathbb{F}_q$ 中每个元素都是平方元, 即 $\mathbb{F}_q^2 = \mathbb{F}_q$. 再设 n 是 $\geqslant 1$ 的整数.

设 $A = (a_{ij})$ 是 $\mathbb{F}_q$ 上的一个对称矩阵, 即满足条件 $a_{ij} = a_{ji}$. 由于 $\mathbb{F}_q$ 的特征数为 2, 所以当 A 的对角线元素 $a_{ii}\,(i = 1, 2, \cdots, n)$ 皆为 0 时, A 是 $\mathbb{F}_q$ 上的一个交错矩阵. 两个 $n \times n$ 对称矩阵 A 和 B 说是合同的, 记作 $A \sim B$, 如果存在 $T \in GL_n(\mathbb{F}_q)$ 使得 $TA\,{}^tT = B$.

令 $S(n, q)$ 表示 $\mathbb{F}_q$ 上全体 $n \times n$ 对称矩阵所成的集合. 显然, 合同关系 $\sim$ 是 $S(n, q)$ 上的一个等价关系. 设 $A = (a_{ij}) \in S(n, q)$, 并设 $\operatorname{rank} A = r$. 如果 A 是 $\mathbb{F}_q$ 上的一个交错矩阵, 那么 r 为偶数. 设 $r = 2s$. 于是

$$A \sim \left[\begin{pmatrix} 0 & I^{(s)} \\ I^{(s)} & 0 \end{pmatrix}, 0^{(n-r)}\right]. \tag{6.1}$$

如果 A 的对角线元素 a_{ii} 不全为 0, 那么, A 可合同于一个对角线矩阵. 设 $A \sim [a_1, \cdots, a_r, 0, \cdots, 0]$, 其中 $a_i \neq 0, i = 1, \cdots, r$. 由于 $\mathbb{F}_q$ 中每个元素皆为平方元, 所以有

$$A \sim [I^{(r)}, 0^{(n-r)}]. \tag{6.2}$$

我们把形如 (6.1) 或 (6.2) 的对称矩阵称为 A 的合同标准形. 值得注意的是, $\mathbb{F}_q$ 上秩为偶数 $2s(> 0)$ 的对称矩阵分为两个合同类, 一个类为交错矩阵的合同类, 另一类为非交错对称矩阵的合同类. 对于 $\mathbb{F}_q$ 上的非交错对称矩阵, 我们也用另外一种标准形. 令

$$S_{2\nu+\delta,\Delta} = \left[\begin{pmatrix} 0 & I^{(\nu)} \\ I^{(\nu)} & 0 \end{pmatrix}, \Delta\right], \tag{6.3}$$

这里 $\nu \geqslant 0, \delta = 0, 1$ 或 2, 而

$$\Delta = \begin{cases} \varnothing\,(\text{不出现}), & \text{如果 } \delta = 0, \\ 1, & \text{如果 } \delta = 1, \\ \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, & \text{如果 } \delta = 2. \end{cases}$$

设 $0 < r \leqslant n$, 且 $r = 2\nu + \delta$, $\delta = 1$ 或 2. 那么容易看出,

$$[I^{(r)}, 0^{(n-r)}] \sim [S_{2\nu+\delta,\Delta}, 0^{(n-r)}]. \tag{6.4}$$

利用 (6.1) 和 (6.4), 我们把含有标准形 $[S_{2\nu+\delta,\Delta}, 0^{(n-2\nu-\delta)}]$ 的 $n\times n$ 对称矩阵的合同类记作 $C_{(2\nu+\delta,\delta)}$.

$S(n, q)$ 对于矩阵加法作成一个交换群, 它的阶为

$$|S(n, q)| = q^{\frac{1}{2}n(n+1)}.$$

$GL_n(\mathbb{F}_q)$ 如下作用在 $S(n, q)$ 上

$$\begin{array}{rcl} GL_n(\mathbb{F}_q)\times S(n, q) & \longrightarrow & S(n, q) \\ (T,\ X) & \longmapsto & TX{}^tT, \end{array} \tag{6.5}$$

那么 $GL_n(\mathbb{F}_q)$ 可看作 $S(n, q)$ 的一个自同构群. 再令 G 为 $GL_n(\mathbb{F}_q)$ 和 $S(n, q)$ 的平移群生成的群. 由定理 1.4, G 就确定了 $S(n, q)$ 上的一个结合方案, 叫做 $\mathbb{F}_q$ 上 n 阶对称矩阵的结合方案, 仍记作 Sym(n, q)(参考本书第五章).

结合方案 Sym(n, q) 的类数等于 $S(n, q)$ 在 $GL_n(\mathbb{F}_q)$ 作用下的非平凡轨道数, 即 $S(n, q)$ 的非平凡的合同类数 $n+[\frac{n}{2}]$. 合同类 $C_{(2s+\tau,\tau)}$ 对应的结合类

$$R_{(2s+\tau,\tau)} = \{(X, Y)|Y-X\in C_{(2s+\tau,\tau)}\}.$$

由于 $\mathbb{F}_q$ 的特征数为 2, $Y-X=X-Y$, 所以 Sym(n, q) 是对称结合方案.

§6.2 结合方案 Sym(n, q) 的非本原性

我们把 Sym(n, q) 的结合类 $R_{(2s+\tau,\tau)}$ 按顺序排成如下形式:

$$R_0,\ R_{(2,0)},\ \cdots,\ R_{(2[\frac{n}{2}],0)},\ R_{(1,1)},\ R_{(2,2)},\ R_{(3,1)},\ \cdots,$$

并且把它们依次记为 $R_0, R_1, \cdots, R_{[\frac{n}{2}]}, R_{[\frac{n}{2}]+1}, R_{[\frac{n}{2}]+2}, \cdots$

令 Y_n 表示 $S(n, q)$ 中交错矩阵的集合. 设 $(P, A)\in G$, 那么 $(P, A)Y_n = Y_n$ 或 $(P, A)(Y_n)\cap Y_n=\varnothing$. 因而 $(G, S(n, q))$ 是非本元的. 由定理 1.18 可知,$(G, S(n, q))$ 确定的结合方案 Sym(n, q) $=(S(n, q), \{R_i\}_{0\leqslant i\leqslant n+[\frac{n}{2}]})$ 是非本原的.

设 $R=\bigcup\limits_{i=0}^{[\frac{n}{2}]} R_i$, $S_1, S_2\in S(n, q)$. 如果 S_1-S_2 是交错矩阵, 就说 S_1 与 S_2 等价. 因而 R 是 $S(n, q)$ 上的一个等价关系. 显然 Y_n 是 R 的一个等价类. 由 §3.1 和 §1.7 知 $\mathcal{Y}_n=(Y_n, \{R_i\}_{0\leqslant i\leqslant[\frac{n}{2}]})$ 是 Sym(n, q) 的一个结合子方案.

我们仍用 $[a_1,\cdots,a_n]$ 表示 $\mathbb{F}_q$ 上 $n\times n$ 对角矩阵, 其对角线上的元素是 a_1, $a_2,\cdots,a_n$. 因为 Y_n 在矩阵的加法下封闭, 所以 Y_n 是 $S(n, q)$ 的一个子群. Y_n 在 $S(n, q)$ 中的所有陪集 $[a_1, a_2, \cdots, a_n]+Y_n$ 恰好是 $S(n, q)$ 中 R 的等价类. 令 $\overline{[a_1, a_2, \cdots, a_n]}$ 表示等价类 $[a_1, a_2, \cdots, a_n]+Y_n$. 那么 $(\overline{[a_1, a_2, \cdots, a_n]}, \{R_i\}_{0\leqslant i\leqslant[\frac{n}{2}]})$

也是 $\mathrm{Sym}(n,\,q)$ 的一个结合子方案，而且这些结合子方案是同构的. 事实上，设 $\overline{[b_1,b_2,\cdots,b_n]}$ 是另一个等价类. 显然，对于 $S\in Y_n$，$[a_1,a_2,\cdots,a_n]+S\longleftrightarrow[b_1,b_2,\cdots,b_n]+S$ 是 $\overline{[a_1,a_2,\cdots,a_n]}$ 和 $\overline{[b_1,b_2,\cdots,b_n]}$ 的一个双射，并且这个双射是这两个等价类之间的一个同构映射.

现在，我们运用定理 1.21 来讨论商结合方案. 我们在指标集 $\{0,\,1,\,\cdots,\,n+[\frac{n}{2}]\}$ 上按如下方法来定义一个等价关系 $\sim$：对于 $i,j\in\{0,\,1,\,\cdots,\,n+[\frac{n}{2}]\}$，如果存在 $\alpha\in\{0,\,1,\,\cdots,\,[\frac{n}{2}]\}$ 使得 $p^j_{i\alpha}\neq0$，就说 $i\sim j$. 显然，$T_0=\{0,\,1,\,\cdots,\,[\frac{n}{2}]\}$ 是 $\sim$ 的一个等价类.

进一步，我们要证明，对于 $[\frac{n}{2}]<i,j\leqslant[\frac{n}{2}]+n$，存在一个 α，$0\leqslant\alpha\leqslant[\frac{n}{2}]$，使得 $p^j_{i\alpha}\neq0$. 因为 $p^j_{i\alpha}\neq0$ 当且仅当 $p^i_{j\alpha}\neq0$，所以可假定 $i\geqslant j$. 我们取 $S_1=0$，$S_2=[1,\cdots1,0,\cdots,0]$，这里 1 的个数是 $j-[\frac{n}{2}]$. 令 $i-j=2s+\tau$，这里 $\tau=0$ 或 1. 设

$$S=\;[I^{(j-[\frac{n}{2}])},\,S_{2s},\,0^{(n-i+[\frac{n}{2}]-2s)}],\quad \text{如果 } \tau=0,$$

或

$$S=\left[I^{(j-1-[\frac{n}{2}])},\,\begin{pmatrix}1&1\\1&0\end{pmatrix},\,S_{2s},\,0^{(n-i+[\frac{n}{2}]-2s-1)}\right],\quad \text{如果 } \tau=1.$$

那么 $(S,S_1)\in R_i$，$(S,S_2)\in R_\alpha$，这里 $\alpha=s$ 或 $s+1$，且 $0\leqslant\alpha\leqslant[\frac{n}{2}]$，因而 $p^j_{i\alpha}\neq0$. 于是 $T_1=\{[\frac{n}{2}]+1,\cdots,[\frac{n}{2}]+n\}$ 是 $\sim$ 的另一个等价类. 因为等价关系 $\sim$ 仅有两个等价类 T_0 和 T_1，所以商结合方案的类数是 1，即这个结合方案是平凡的.

综合上面的讨论，我们有

定理 6.1 (i) 结合方案 $\mathrm{Sym}(n,\,q)=(S(n,\,q),\{R_i\}|_{0\leqslant i\leqslant n+[\frac{n}{2}]})$ 是非本原的.

(ii) $R=\bigcup\limits_{i=0}^{[\frac{n}{2}]}R_i$ 是 $S(n,\,q)$ 的一个等价关系，$\Sigma:=\{\overline{(a_1,\cdots,a_n)}|a_i\in\mathbb{F}_q\}$ 是它的非本原系.

(iii) 这些结合子方案 $(\overline{(a_1,\cdots,a_n)},\,\{R_i\}_{0\leqslant i\leqslant[\frac{n}{2}]})$ 彼此同构.

(iv) 商结合方案 $\mathrm{Sym}(n,\,q)/\Sigma$(也即从 $(G,\,\Sigma)$ 得到的结合方案) 的类数是 1(即 $(G,\,\Sigma)$) 是双可迁的).

§6.3 结合方案 Sym(2, q)

容易看出，结合方案 $\mathrm{Sym}(1,\,q)$ 是平凡的. 现在来看 $\mathrm{Sym}(2,\,q)$. 这时，$n=2$，$|S(2,\,q)|=q^3$. $S(2,\,q)$ 的合同类有 4 个：$C_0=\{0^{(2)}\}$，$C_{(1,1)}$，$C_{(2,2)}$，$C_{(2,0)}$. 对应的结合类为 $R_0,R_{(1,1)},R_{(2,2)},R_{(2,0)}$. 我们将这 4 个结合类依次记为 R_0，R_1，R_2，R_3，对应的价记为 k_0，k_1，k_2，k_3. 简单计算可知

$$k_0=1,\,k_1=q^2-1,\,k_2=(q-1)(q^2-1),\,k_3=q-1.$$

我们不难计算 Sym(2, q) 的交叉数 p_{ij}^k. 例如我们计算 p_{11}^1. 令

$$S_1 = 0,\ \ S_2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

并且设

$$\mathcal{M} = \{S \in S(2, q) | (S, S_1), (S, S_2) \in R_1\},$$

那么 $p_{11}^1 = |\mathcal{M}|$. 设 $S = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$, 那么 $S \in \mathcal{M}$ 当且仅当

$$\operatorname{rank} \begin{pmatrix} a & b \\ b & d \end{pmatrix} = \operatorname{rank} \begin{pmatrix} a-1 & b \\ b & d \end{pmatrix} = 1.$$

由此可知 $ad - b^2 = 0$, $(a-1)d - b^2 = 0$. 所以 $d = 0$, $b = 0$, $a \neq 0, 1$. 因而

$$\mathcal{M} = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} | a \in \mathbb{F}_q,\ a \neq 0,\ 1 \right\}.$$

于是 $p_{11}^1 = q - 2$.

类似地, 可以算出 $p_{11}^2 = q$, $p_{11}^3 = 0$ 等等.

我们计算出 Sym(2, q) 的三个交叉矩阵为

$$B_1 = (p_{1j}^k) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ q^2-1 & q-2 & q & 0 \\ 0 & q(q-1) & (q-2)(q+1) & q^2-1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \tag{6.6}$$

$$B_2 = (p_{2j}^k) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & q(q-1) & (q-2)(q+1) & q^2-1 \\ (q-1)(q^2-1) & (q-2)(q^2-1) & q^3-2q^2-q+4 & (q-2)(q^2-1) \\ 0 & q-1 & q-2 & 0 \end{pmatrix},$$

$$B_3 = (p_{3j}^k) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & q-1 & q-2 & 0 \\ q-1 & 0 & 0 & q-2 \end{pmatrix}.$$

因为 B_1 是三对角线矩阵, 并且其旁对角线上的元素非零, 所以由定理 1.23, Sym(2,q) 是 P 多项式结合方案. 进一步, 我们有

定理 6.2 Sym(2, q) 关于顺序 R_0, R_1, R_2, R_3 是 P 多项式结合方案, 交叉矩阵 B_1 的特征值是

$$\theta_0 = q^2 - 1,\ \theta_1 = q - 1,\ \theta_2 = -1 \text{ 和 } \theta_3 = -q - 1,$$

它们对应的重数分别是

$$m_0 = 1, m_1 = \frac{1}{2}q(q^2-1), m_2 = q^2-1 \text{ 和 } m_3 = \frac{1}{2}q(q-1)^2.$$

此外,Sym(2, q) 的第一特征值矩阵是

$$P = (p_i(j)) = \begin{pmatrix} 1 & q^2-1 & (q-1)(q^2-1) & q-1 \\ 1 & q-1 & 1-q & -1 \\ 1 & -1 & 1-q & q-1 \\ 1 & -q-1 & q+1 & -1 \end{pmatrix}, \tag{6.7}$$

第二特征值矩阵是

$$Q = \begin{pmatrix} 1 & \frac{1}{2}q(q^2-1) & q^2-1 & \frac{1}{2}q(q-1)^2 \\ 1 & \frac{1}{2}q(q-1) & -1 & -\frac{1}{2}q(q-1) \\ 1 & -\frac{1}{2}q & -1 & \frac{1}{2}q \\ 1 & -\frac{1}{2}q(q+1) & q^2-1 & -\frac{1}{2}q(q-1) \end{pmatrix}. \tag{6.8}$$

当 $q \neq 2$ 时, Sym(2, q) 不是自对偶的.

证明 参看定理 1.23 的证明, 我们从 (6.6) 得到

$$\begin{aligned} v_0(x) = 1,\ v_1(x) &= x,\ qv_2(x) = x^2-(q-2)x-(q^2-1), \\ q(q^2-1)v_3(x) &= x^3-(q^2-4)x^2-(3q^2-5)x+(q-2)(q+1)(q^2-1). \end{aligned}$$

进而有 $q(q^2-1)\sum_{i=0}^{3} v_i(x) = x^3+3x^2-(q^2-3)x-(q^2-1)$. 因此 B_1 的特征多项式是

$$(x-(q^2-1))(x^3+3x^2-(q^2-3)x-(q^2-1)).$$

分解这个多项式, 就得到 B_1 的特征值. 从 $p_i(j) = v_i(\theta_j)\ (i, j = 0, 1, 2$ 或 $3)$, 我们得到 (6.7).

再由关系式 $PQ = QP = |X|I$ 即可得出 (6.8), 从而得到重数 m_i ($i = 0, 1, 2,$ 或 3). 注意到, 当 $q \neq 2$ 时, 交换 Q 的行 (列) 不能得到 P, 所以 Sym(2, q) 不是自对偶的.□

进一步, 我们还有

定理 6.3 当 q 是 2 的幂, 并且 $\mathbb{F}_q \neq \mathbb{F}_2$ 时,Sym$(2, q)$ 关于 R_0, R_1, R_2, R_3 的任何顺序都不是 Q 多项式方案; 而在 $\mathbb{F}_q = \mathbb{F}_2$ 时 Sym(2, q) 关于顺序 R_0, R_1, R_2, R_3 是 (P 和 Q) 多项式方案.

证明 我们从 (6.7) 和等式

$$q_{ij}^k = \frac{m_i m_j}{|X|} \sum_{l=0}^{s} \frac{1}{k_l^2} p_l(i) p_l(j) \bar{p}_l(k).$$

可以算出 Sym(2, q) 的 Krein 参数 q_{ij}^k, 从而得到 Sym(2, q) 的如下 Krein 参数矩阵

$$\hat{B}_1=(q_{1j}^k)=\begin{pmatrix} 0 & 1 & 0 & 0 \\ \dfrac{q(q^2-1)}{2} & \dfrac{q(q-2)(q+3)}{4} & \dfrac{q(q-1)(q+2)}{4} & \dfrac{q(q+1)(q-2)}{4} \\ 0 & \dfrac{(q-1)(q+2)}{2} & 0 & \dfrac{q(q+1)}{2} \\ 0 & \dfrac{q(q-1)(q-2)}{4} & \dfrac{q^2(q-1)}{4} & \dfrac{q(q+1)(q-2)}{4} \end{pmatrix},$$

$$\hat{B}_2=(q_{2j}^k)=\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & \dfrac{(q-1)(q+2)}{2} & 0 & \dfrac{q(q+1)}{2} \\ q^2-1 & 0 & q^2-2 & 0 \\ 0 & \dfrac{q(q-1)}{2} & 0 & \dfrac{(q+1)(q-2)}{2} \end{pmatrix},$$

$$\hat{B}_3=(q_{3j}^k)=\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & \dfrac{q(q-1)(q-2)}{4} & \dfrac{q^2(q-1)}{4} & \dfrac{q(q+1)(q-2)}{4} \\ 0 & \dfrac{q(q-1)}{2} & 0 & \dfrac{(q+1)(q-2)}{2} \\ \dfrac{q(q-1)^2}{2} & \dfrac{q(q-1)(q-2)}{4} & \dfrac{q(q-1)(q-2)}{4} & \dfrac{q(q-2)(q-3)}{4} \end{pmatrix}.$$

当 $\mathbb{F}_q \neq \mathbb{F}_2$ 时, $\hat{B}_1$ 的第二列和 $\hat{B}_3$ 的第四列都有 4 个非零元素, 而 $\hat{B}_2$ 的第三列除了 (3,3) 位置的元素外, 只有一个非零元素. 所以所有 $\hat{B}_i(i=1,2,3)$ 都不是其旁对角线上元素非零的三对角线矩阵.

当 $\mathbb{F}_q = \mathbb{F}_2$ 时,

$$\hat{B}_1=\begin{pmatrix} 0 & 1 & 0 & 0 \\ 3 & 0 & 2 & 0 \\ 0 & 2 & 0 & 3 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

是三对角线矩阵, 其旁对角线上的元素非零. 由定理 1.26, 除去 $\mathbb{F}_q = \mathbb{F}_2$, Sym (2, q) 不是 Q 多项式结合方案, 而在 $\mathbb{F}_q = \mathbb{F}_2$ 时, Sym (2, q) 是 P 和 Q 多项式结合方案, 并且同构于立方体方案. □

下面证明, 当 $n \geqslant 3$ 时, Sym (n, q) 也不是 P 多项式的.

我们对 n 施行数学归纳法来讨论 Sym (n, q) 的多项式性质.

我们把 Sym (n, q) 的结合关系 $R_{(2i+\tau,\tau)}$ 记为 $R_{(2i+\tau,\tau)}(n)$, 并且用 $B_{(2i+\tau,\tau)}$ 来表示对应于结合关系 $R_{(2i+\tau,\tau)}(n)$ 的交叉矩阵. 我们要证明：当 $n \geqslant 3$ 时 Sym(n, q) 不是 P 多项式结合方案. 为了证明这个断言, 由定理 1.23, 只需证明在结合关系

$R_{(2i+\tau,\tau)}(n)$ 的任意排列的顺序下, 其第一个关系 (譬如 $R_{(2i+\tau,\tau)}(n)$) 所对应的矩阵 ($B_{(2i+\tau,\tau)}$) 不是三对角线矩阵而且其旁对角线上的元素非零, 这里 $1 \leqslant 2i+\tau \leqslant n$, $\tau = 0, 1$, 或 2. 我们用以下的两种方法来证明这个断言:

i) 如果选取一个 $(2j+\mu, \mu)$, 使得 $p^{(2j+\mu,\mu)}_{(2i+\tau,\tau)(*,*)}(n) \neq 0$, 其中 $(*, *)$ 是不同于 $(2j+\mu,\mu)$ 的三种选取, 那么在 $B_{(2i+\tau,\tau)}$ 的第 $(2j+\mu,\mu)$ 列除了 $((2j+\mu,\mu),(2j+\mu,\mu))$ 的位置上的元素外, 还有 3 个不为零的元素, 因而 $B_{(2i+\tau,\tau)}$ 不是三对角线矩阵;

ii) 如果选取一个 $(2j+\mu, \mu)$, 使得对于不同于 $(2j+\mu, \mu)$ 两种选取 $(2k+\lambda,\lambda)$ 和 $(2k'+\lambda', \lambda')$, 有 $p^{(2j+\mu,\mu)}_{(2i+\tau)(2k+\lambda,\lambda)}(n) \neq 0$, $p^{(2j+\mu,\mu)}_{(2i+\tau,\tau)(2k'+\lambda',\lambda')}(n) \neq 0$ 和 $p^{(2k+\lambda,\lambda)}_{(2i+\tau,\tau)(2k'+\lambda',\lambda')}(n) \neq 0$, 那么 $B_{(2i+\tau,\tau)}$ 也不是三对角线矩阵, 而且其旁对角线上的元素非零. 不然, 如果 $B_{(2i+\tau,\tau)}$ 是三对角线矩阵, 而且其旁对角线上的元素非零, 那么从前两个非零交叉数可知, 在给定的结合关系排列的顺序下, $R_{(2j+\mu,\mu)}(n)$ 在 $R_{(2k+\lambda,\lambda)}(n)$ 和 $R_{(2k'+\lambda',\lambda')}(n)$ 之间, 而第三个非零交叉数说明,$R_{(2k+\lambda,\lambda)}(n)$ 和 $R_{(2k'+\lambda',\lambda')}(n)$ 必需相邻, 这是一个矛盾.

下面讨论中的第一关系是在给定的结合关系排列的顺序下说的. 我们用上述的步骤 i) 和 ii) 来讨论 Sym$(3, q)$ 的情形,

(a) $R_{(1,1)}(3)$ 是第一关系.

令 $S_1 = 0$, $S_2 = E_{12} + E_{21} + E_{22}$, 并且取 $S = E_{11}$, E_{12} 和 E_{33}, 那么 $(*, *)$ 分别是 $(1, 1)$, $(2, 0)$ 和 $(3,1)$, 使得 $p^{(2,2)}_{(1,1)(*,*)}(3) \neq 0$. 由 i) 可知 $B_{(1,1)}$ 不是三对角线矩阵.

(b) $R_{(2,2)}(3)$ 是第一关系

令 $S_1 = 0$, $S_2 = E_{11} + E_{22} + E_{33}$, 并且取

$$S = \begin{pmatrix} 1 & & \\ & 1 & \\ & & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & \\ 1 & 1 & \\ & & 1 \end{pmatrix} \text{和} \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix},$$

那么 $(*, *)$ 分别是 $(1,1), (2,0)$ 和 $(2,2)$, 使得 $p^{(3,1)}_{(2,2)(*,*)}(3) \neq 0$. 仍由 i) 可知 $B_{(2,2)}$ 不是三对角线矩阵.

(c) $R_{(3,1)}(3)$ 是第一关系.

令 $S_1 = 0$, $S_2 = E_{11}$, 并且取 $S = E_{11} + E_{23} + E_{32}, E_{11} + E_{22} + E_{33}$ 和 $E_{12} + E_{21} + E_{33}$, 那么 $(*, *)$ 分别是 $(2,0), (2,2)$ 和 (3,1), 使得 $p^{(1,1)}_{(3,1)(*,*)}(3) \neq 0$. 因而 $B_{(3,1)}$ 不是三对角线矩阵.

(d) $R_{(2,0)}(3)$ 是第一关系.

令 $S_1 = 0$, $S_2 = E_{11}$, 并且取 $S = E_{12} + E_{21}$ 和 $E_{23} + E_{32}$, 那么 $p^{(1,1)}_{(2,0)(2,2)}(3) \neq 0$ 和 $p^{(1,1)}_{(2,0)(3,1)}(3) \neq 0$. 然而, 如果取 $S_1 = 0$, $S_2 = E_{11} + E_{22}$ 和 $S = E_{23} + E_{32}$, 就有 $p^{(2,2)}_{(2,0)(3,1)}(3) \neq 0$. 由 ii) 可知 $B_{(2,0)}$ 不是三对角线矩阵, 而其旁对角线上的元素非零.

综合上述四种情形, 我们就得到 Sym$(3, q)$ 不是 P 多项式方案.

现在证明 Sym (4, q) 不是 P 多项式方案. 对于任意 $S \in S(3, q)$, 令

$$\widetilde{S} = [S,\ 0] \in S(4, q),$$

就可用这种方法把 $S(3, q)$ 嵌入到 $S(4, q)$ 中, 所以, 对于满足 $2i + \tau < 4$ 的任意 $(2i + \tau, \tau)$, 根据对 Sym (3, q) 的证明, 可以证明:"对于结合关系 $R_{(2i+\tau,\tau)}(4)$ 的任一排列顺序下, Sym(4, q) 的 $B_{(2i+\tau,\tau)}$ 不是三对角线的.

我们来考虑 $R_{(4,0)}(4)$ 和 $R_{(4,2)}(4)$. 先讨论在结合关系的排列顺序下 $R_{(4,2)}(4)$ 为第一关系. 令 $S_1 = 0$, $S_2 = E_{11} + E_{22}$, 并且取

$$S = \left[1, 1, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right], \left[1, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, 1\right] \text{ 和 } \left[\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, 1, 1\right],$$

那么 $(*, *)$ 分别取 (2, 0), (3, 1) 和 (4, 2), 使得 $p^{(2,2)}_{(4,2)(*,*)}(4) \neq 0$. 因而 $B_{(4,2)}$ 不是三对角线矩阵.

我们再讨论在结合关系的给定排列顺序下 $R_{(4,0)}(4)$ 是第一关系. 令 $S_1 = 0$, $S_2 = E_{12} + E_{21} + E_{22}$, 并且取 $S = E_{12} + E_{21} + E_{34} + E_{43}$ 和 $E_{13} + E_{31} + E_{24} + E_{42}$, 那么 $p^{(2,2)}_{(4,0)(3,1)}(4) \neq 0$ 和 $p^{(2,2)}_{(4,0)(4,2)}(4) \neq 0$. 然而, 如果令 $S_1 = 0$, $S_2 = E_{13} + E_{31} + E_{44}$, 并且取 $S = E_{12} + E_{21} + E_{34} + E_{43}$, 那么 $p^{(3,1)}_{(4,0)(4,2)}(4) \neq 0$, 因而 $B_{(4,0)}$ 不是三对角线矩阵.

由上讨论可知, Sym (4, q) 不是 P 多项式方案.

现在假定 $n \geqslant 5$ 并且对于所有 $k \leqslant n$, Sym (k, q) 不是 P 多项式的. 如同讨论 Sym (4, q) 的一样, 我们可以把 Sym ($n - 1$, q) 嵌入到 Sym (n, q) 中, 因此由归纳假设, 对于满足 $2i + \tau < n$ 的任意 $(2i + \tau, \tau)$, $B_{(2i+\tau,\tau)}$ 不是三对角线矩阵.

我们来讨论 $2i + \tau = n$ 的情形, 我们要区分 n 是奇数或偶数两种情形. 如果 n 是奇数, 就令 $n = 2i + 1$,

$$S_1 = 0 \text{ 和 } S = \left[\begin{pmatrix} 0 & I^{(i-1)} \\ I^{(i-1)} & 0 \end{pmatrix}, W\right],$$

这里 W 是秩为 3 的 3×3 的矩阵, 考虑矩阵右下角的 3×3 块, 就可按照对 Sym (3, q) 所做的步骤进行, 从而得到 $B_{(2i+\tau,\tau)}$ 不是三对角线矩阵.

如果 n 是偶数, 就令 $n = 2i + 2$,

$$S_1 = 0 \text{ 和 } S = \left[\begin{pmatrix} 0 & I^{(i-1)} \\ I^{(i-1)} & 0 \end{pmatrix}, W\right],$$

这里 W 是秩为 4 的 4×4 的矩阵, 仍考虑矩阵右下角的 4×4 块, 就可按照对 Sym (4, q) 所做的步骤进行, 从而得到 $B_{(2i+\tau,\tau)}$ 不是三对角线矩阵, 这里 $\tau = 0$ 或 2.

因此, 当 $n \geqslant 5$ 时, $\mathrm{Sym}\,(n, q)$ 不是 P 多项式结合方案.

我们把上述的结果写成如下的

定理 6.3′ 设 $n \geqslant 3$, 那么 $\mathrm{Sym}\,(n, q)$ 不是 P 多项式结合方案.

§6.4 伪辛空间的一些结果

在后面的几节中, 我们要讨论 $n \geqslant 3$ 时 $\mathrm{Sym}(n, q)$ 的参数计算. 由于 q 为偶数时,$S(n, q)$ 含有交错矩阵, 所以在计算中, 除了引用辛空间的一些结果外, 还要引用 [15] 中建立起来的关于伪辛空间的一些结果.

所谓伪辛群是由 $\mathbb{F}_q$ 上一个满秩非交错对称矩阵定义的群. 设 n 为 $\geqslant 1$ 的整数, 并设 $n = 2\nu + \delta$, 这里 $\delta = 0, 1$, 或 2. 为了简单, 有时记

$$S_{2\nu+\delta} = [S_{2\nu}, \Delta],$$

这里

$$S_{2\nu} = \begin{pmatrix} 0 & I^{(\nu)} \\ I^{(\nu)} & 0 \end{pmatrix}, \quad \Delta = \begin{cases} \varnothing, & \text{如果 } \delta = 0, \\ 1, & \text{如果 } \delta = 1, \\ \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, & \text{如果 } \delta = 2. \end{cases} \tag{6.9}$$

$\mathbb{F}_q$ 上满足

$$T S_{2\nu+\delta}\, {}^tT = S_{2\nu+\delta}$$

的全体 $n \times n$ 矩阵 T 对于矩阵的乘法作成 $GL_n(\mathbb{F}_q)$ 的一个子群. 当 $\delta = 0$ 时, 这个子群就是第三章所述的辛群 $Sp_{2\nu}(\mathbb{F}_q)$; 当 $\delta = 1$ 或 2 时, 这个子群称为 $\mathbb{F}_q$ 上关于 $S_{2\nu+\delta}$ 的伪辛群, 记作 $Ps_{2\nu+\delta}(\mathbb{F}_q)$, 而且把 T 称为关于 $S_{2\nu+\delta}$ 的伪辛矩阵.

当 $\delta = 1$ 或 2 时, 由 [15] 中的定理 4.7, $Ps_{2\nu+\delta}(\mathbb{F}_q)$ 的阶为

$$|Ps_{2\nu+\delta}(\mathbb{F}_q)| = q^{(\nu+\delta-1)^2} \prod_{i=1}^{\nu} (q^{2i} - 1). \tag{6.10}$$

$Ps_{2\nu+1}(\mathbb{F}_q)$ 由全体形如

$$[T, 1] \tag{6.11}$$

的矩阵组成, 这里 $T \in Sp_{2\nu}(\mathbb{F}_q)$. 所以 $Ps_{2\nu+1}(\mathbb{F}_q)$ 同构于辛群 $Sp_{2\nu}(\mathbb{F}_q)$. 而 $Ps_{2\nu+2}(\mathbb{F}_q)$ 由全体形如

$$\begin{matrix} \begin{pmatrix} T & TS_{2\nu}\,{}^tc & 0 \\ 0 & 1 & 0 \\ c & d & 1 \end{pmatrix} & \begin{matrix} 2\nu \\ 1 \\ 1 \end{matrix} \\ \begin{matrix} 2\nu \quad\quad & 1 \quad\quad & 1 \end{matrix} & \end{matrix} \tag{6.12}$$

的矩阵组成, 这里 $T \in Sp_{2\nu}(\mathbb{F}_q)$, $c \in \mathbb{F}_q^{(2\nu)}$, d 是 $\mathbb{F}_q$ 中的任意元素.

注意到,$TS_{2\nu+\delta}{}^tT = S_{2\nu+\delta} \Leftrightarrow {}^tTS_{2\nu+\delta}^{-1}T = S_{2\nu+\delta}^{-1}$. 所以当 $\delta = 1$ 时, 如果 $T \in Ps_{2\nu+1}(\mathbb{F}_q)$, 那么 ${}^tT \in Ps_{2\nu+1}(\mathbb{F}_q)$. 但对于 $\delta = 2$ 时, 如果 $P \in Ps_{2\nu+2}(\mathbb{F}_q)$, 那么有

$$
{}^tT\left[S_{2\nu}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\right]T = \left[S_{2\nu}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\right].
$$

设 $\mathbb{F}_q^{(n)}$ 是 $\mathbb{F}_q$ 上的 n 维行向量空间,$\{e_i|1 \leqslant i \leqslant n\}$ 是它的一组基. 当 $\delta = 1$ 或 2 时,$\mathbb{F}_q^{(2\nu+\delta)}$ 连同 $Ps_{2\nu+\delta}(\mathbb{F}_q)$ 在它上面的作用称为 (由 $S_{2\nu+\delta}$ 决定的)伪辛空间. 因为伪辛矩阵在 $\mathbb{F}_q^{(2\nu+\delta)}$ 上的作用是线性的, 因而它自然地作用在 $\mathbb{F}_q^{(2\nu+\delta)}$ 的子空间的集合上.

设 P 是 $\mathbb{F}_q^{(2\nu+\delta)}$ 的一个 m 维子空间, 仍用 P 作为子空间 P 的矩阵表示. 当 $\delta = 0$ 时已在 §3.2 中讨论过, 这里不再多叙. 下面假定 $\delta = 1$ 或 2. 如果 $Ps_{2\nu+\delta}{}^tP \sim [S_{2s}, \Lambda, 0^{(m-2s-\tau)}]$, 这里 $\tau = 0$, 1, 或 2, 而 Λ 由 (6.9) 确定, 并令 $\epsilon = 0$ 或 1 分别由 $e_{2\nu+1} \notin P$ 或 $e_{2\nu+1} \in P$ 来确定, 那么就称 P 是关于 $S_{2\nu+\delta}$ 的$(m,\ 2s+\tau,\ s,\ \varepsilon)$ 型子空间.

在 $(2\nu+\delta)$ 维伪辛空间中,$(m,\ 2s+\tau,\ s,\ \varepsilon)$ 型子空间存在, 当且仅当

$$
(\tau, \varepsilon) = \begin{cases} (0,0),\ (1,0),\ (1,1),\ \text{或}\ (2,0), & \text{如果}\ \delta = 1, \\ (0,0),\ (0,1),\ (1,0),\ (2,0),\ \text{或}\ (2,1), & \text{如果}\ \delta = 2 \end{cases} \tag{6.13}
$$

和

$$
2s + \max\{\tau,\ \varepsilon\} \leqslant m \leqslant \nu + s + [(\tau + \delta - 1)/2] + \varepsilon. \tag{6.14}
$$

设 $N(m,\ 2s+\tau,\ s, \varepsilon;\ 2\nu+\delta)$ 表示 $(2\nu+\delta)$ 维伪辛空间中 $(m,\ 2s+\tau,\ s,\ \varepsilon)$ 型子空间的个数,[15] 中证明了

$$
\begin{aligned}
&N(m,\ 2s+\tau,\ s,\ \varepsilon; 2\nu+\delta) \\
&\quad = q^{n_0+2(s+(2-\delta)[\tau/2])(\nu+s-m+\delta[(\tau+1)/2]+(\delta-1)(\tau-1)(\tau-2)\varepsilon/2)} \\
&\quad \cdot \frac{\prod\limits_{i=\nu+s-m+[(\tau+\delta-1)/2]+\varepsilon+1}^{\nu} (q^{2i}-1)}{\prod\limits_{i=1}^{s}(q^{2i}-1) \prod\limits_{i=1}^{m-2s-\max\{\tau,\varepsilon\}} (q^i-1)},
\end{aligned} \tag{6.15}
$$

这里 $n_0 = 0$ 如果 $\delta = 1$; 而当 $\delta = 2$ 时, n_0 分别为

$$
n_0 = \begin{cases} m, & \text{如果}\ (\tau,\ \epsilon) = (0,\ 0), \\ 0, & \text{如果}\ (\tau,\ \epsilon) = (0,\ 1), \\ 2(\nu+1)-m, & \text{如果}\ (\tau,\ \epsilon) = (1,\ 0),\ (2,\ 0)\ \text{或}\ (2,\ 1). \end{cases}
$$

利用伪辛空间中的这个公式, 我们可以得到 $\mathbb{F}_q$ 上某些矩阵类的计数公式.

$\mathbb{F}_q$ 上的 $l\times(2\nu+\delta)$ 矩阵 U 说成是关于 $S_{2\nu+\delta}$ 的$(l, m, 2s+\tau, s, \epsilon)$ 型矩阵, 如果由 U 的行向量张成的子空间是关于 $S_{2\nu+\delta}$ 的 $(m, 2s+\tau, s, \epsilon)$ 型子空间. 我们记关于 $S_{2\nu+\delta}$ 的 $(l, m, 2s+\tau, s, \varepsilon)$ 型矩阵的个数为 $n(l, m, 2s+\tau, s, \varepsilon; 2\nu+\delta)$. 那么有

定理 6.4 设 $n=2\nu+\delta$, $\delta=1$, 或 2. 那么

$$\begin{aligned} &n(l, m, 2s+\tau, s, \epsilon; 2\nu+\delta)\\ =&q^{\frac{1}{2}m(m-1)}N(m, 2s+\tau, s, \epsilon; 2\nu+\delta)\prod_{i=l-m+1}^{l}(q^i-1). \end{aligned} \tag{6.16}$$

证明 设 U 是 $\mathbb{F}_q^{(2\nu+\delta)}$ 的一个 m 维子空间, 我们取 U 的一个基 $u_1, \cdots, u_m$. 那么 $l\times n$ 矩阵 Q 的行向量生成 U 当且仅当存在一个秩为 m 的 $l\times m$ 矩阵 M, 使得 $Q=M\,{}^t({}^tu_1, \cdots, {}^tu_m)$. 此外, 不同的 M 给出不同的 Q. 由 (1.5) 可知,$\mathbb{F}_q$ 上秩为 m 的 $l\times m$ 矩阵的个数是

$$q^{\frac{1}{2}m(m-1)}\prod_{i=l-m+1}^{l}(q^i-1),$$

因此 (6.16) 成立. □

应用伪辛群的阶之公式, 我们容易给出 $\mathbb{F}_q$ 上对称矩阵的合同类 $C_{(2s+\tau,\tau)}$的计数公式. 将结合方案 $\mathrm{Sym}(n,q)$ 中对应于结合关系 $R_{(2s+\tau,\tau)}$ 的价记为 $k_{(2s+\tau,\tau)}(n)$, 于是 $k_{(2s+\tau,\,\tau)}(n)=|C_{(2s+\tau,\,\tau)}|$. 令

$$M(n,\, 2s+\tau,\, \tau)=[S_{2s+\tau,\,\Lambda},\, 0^{(n-2s-\tau)}].$$

我们有

定理 6.5 $\mathbb{F}_q$ 上合同于标准形 $M(n,\, 2s+\tau,\, \tau)$ 的 $n\times n$ 对称矩阵的个数为

$$k_{(2s+\tau,\,\tau)}(n)=|C_{(2s+\tau,\,\tau)}|=\begin{cases} q^{s(s-1)}\dfrac{\prod\limits_{j=n-2s+1}^{n}(q^j-1)}{\prod\limits_{j=1}^{s}(q^{2j}-1)}, & \text{如果 } \tau=0,\\ q^{s(s+1)}\dfrac{\prod\limits_{j=n-2s-\tau+1}^{n}(q^j-1)}{\prod_{j=1}^{s}(q^{2j}-1)}, & \text{如果 } \tau=1 \text{ 或 } 2. \end{cases} \tag{6.17}$$

证明 当 $\tau=0$ 时, 此即 $\mathbb{F}_q$ 上秩为 $2s$ 的 n 阶交错矩阵的计数公式 (3.13). 下面设 $\tau=1$ 或 2. $C_{(2s+\tau,\,\tau)}$ 是 $GL_n(\mathbb{F}_q)$ 作用在 $S(n,\, q)$ 上含有标准形 $M(n,\, 2s+\tau,\, \tau)$ 的轨道. 设 $M(n,\, 2s+\tau,\, \tau)$ 在 $GL_n(\mathbb{F}_q)$ 中的稳定子记作 $G_{S_{2s+\tau}}$. 那么 $G_{S_{2s+\tau}}$ 由 $GL_n(\mathbb{F}_q)$ 中满足条件

$$TM(n,\, 2s+\tau,\, \tau)\,{}^tT=M(n,\, 2s+\tau,\, \tau)$$

的全体矩阵组成. 将 T 相应于 $M(n,\, 2s+\tau,\, \tau)$ 分块,

$$T = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{matrix} 2s+\tau \\ n-2s-\tau \end{matrix},$$
$$\qquad\quad 2s+\tau \quad n-2s-\tau$$

这样就有下面的等式:

$$AS_{2s+\tau}\,{}^tA = S_{2s+\tau},\quad AS_{2s+\tau}\,{}^tC = 0.$$

由此可知,$A \in Ps_{2s+\tau}(\mathbb{F}_q)$, 特别是 A 非奇异. 所以 $C=0$, $D \in GL_{n-2s-\tau}(\mathbb{F}_q)$, 而 B 是 $\mathbb{F}_q$ 上任意 $(2s+\tau)\times(n-2s-\tau)$ 矩阵. 因而

$$|G_{S_{2s+\tau}}| = |Ps_{2s+\tau}(\mathbb{F}_q)| \cdot |GL_{n-2s-\tau}(\mathbb{F}_q)| q^{(2s+\tau)(n-2s-\tau)}.$$

于是

$$|C_{(2s+\tau,\tau)}| = \frac{|GL_n(\mathbb{F}_q)|}{|Ps_{2s+\tau}(\mathbb{F}_q)||GL_{n-2s-\tau}(\mathbb{F}_q)|q^{(2s+\tau)(n-2s-\tau)}}.$$

应用公式 (6.10) 和 (2.2), 对上式整理即得本定理中的结果. □

§6.5 交叉数 p^*_{**} 的递推计算

我们把结合方案 Sym$(n,\, q)$ 的交叉数记为 $p^{(2k+\lambda,\,\lambda)}_{(2i+\tau,\,\tau)(2j+\mu,\,\mu)}(n)$, 给出它们的一种递推计算. 下面总设 $n \geqslant 3$. 我们分 $2i+\tau$, $2j+\mu$ 和 $2k+\lambda$ 中至少有一个小于 n 和它们三个全等于 n 两种情形.

本节中设 $2i+\tau$, $2j+\mu$ 和 $2k+\lambda$ 中至少有一个小于 n. 由命题 1.1, 不妨设 $2k+\lambda<n$. 因为两个交错矩阵的差仍是交错矩阵, 所以当 λ, τ, μ 中有两个为 0 而第三个不为 0 时, 就有 $p^{(2k+\lambda,\lambda)}_{(2i+\tau,\tau)(2j+\mu,\mu)}(n)=0$. 再由 Sym$(n,\, q)$ 的对称性和命题 1.1, 我们只需要考虑 $(\lambda,\, \tau,\, \mu)$ 取如下 8 种情形:

$$(0,0,0), (0,1,1), (0,1,2), (0,2,2), (1,1,1), (1,1,2), (1,2,2) \text{ 和 } (2,2,2).$$

对于 $(\lambda,\tau,\mu)=(0,0,0)$ 的情形, 已有定理 3.10 给出 $p^{(k,0)}_{(i,0)(j,0)}(n)$ 的递推公式. 于是只需考虑 $(\lambda,\, \tau,\, \mu)$ 取其余的 7 种情形.

令 $S_1 = 0^{(n)}$, $S_2 = M(n,\, 2k+\lambda,\, \lambda)$ 和

$$\mathcal{M} = \{S \in S(n,\, q) | (S,\, S_1) \in R_{(2i+\tau,\tau)}, (S,\, S_2) \in R_{(2j+\mu,\mu)}\}.$$

那么

$$p^{(2k+\lambda,\lambda)}_{(2i+\tau,\tau)(2j+\mu,\mu)}(n) = |\mathcal{M}|. \tag{6.18}$$

设 G_0 是 G 的子群，它使 S_1 和 S_2 不动，那么 G_0 保持 $\mathcal{M}$ 不变，并且可以看作 $GL_n(\mathbb{F}_q)$ 的子群，它由所有形如

$$\begin{pmatrix} R & Q \\ 0 & T \end{pmatrix} \begin{matrix} 2k+\lambda \\ n-2k-\lambda \end{matrix}$$
$$\begin{matrix} 2k+\lambda & n-2k-\lambda \end{matrix}$$

的矩阵组成，其中 R 满足 $RM(2k+\lambda, 2k+\lambda, \lambda)\,{}^tR = M(2k+\lambda, 2k+\lambda, \lambda)$, $T \in GL_{n-2k-\lambda}(\mathbb{F}_q), Q$ 是 $\mathbb{F}_q$ 上的 $(2k+\lambda)\times(n-2k-\lambda)$ 矩阵. 我们把 $\mathcal{M}$ 中的矩阵 S 写成分块矩阵形式

$$\begin{pmatrix} U & {}^tV \\ V & W \end{pmatrix} \begin{matrix} 2k+\lambda \\ n-2k-\lambda \end{matrix}.$$
$$\begin{matrix} 2k+\lambda & n-2k-\lambda \end{matrix}$$

设

$$\mathcal{M}(2t+\rho, \rho) = \left\{ S = \begin{pmatrix} U & {}^tV \\ V & W \end{pmatrix} \in \mathcal{M} | W \sim M(n-2k-\lambda, 2t+\rho, \rho) \right\},$$

这里 t, ρ 满足

$$0 \leqslant 2t+\rho \leqslant n-2k-\lambda,\ \rho = 0, 1 \text{ 或 } 2. \tag{6.19}$$

那么

$$|\mathcal{M}| = \sum_{t,\rho\text{满足}(6.19)} |\mathcal{M}(2t+\rho, \rho)|. \tag{6.20}$$

为了简单起见，记 $M_{(t,\rho)} = M(2t+\rho, 2t+\rho, \rho)$，并且令

$$\mathcal{M}_1 = \left\{ \begin{pmatrix} U & {}^tV_1 & {}^tV_2 \\ V_1 & M_{(t,\rho)} & 0 \\ V_2 & 0 & 0 \end{pmatrix} \in \mathcal{M}(2t+\rho, \rho) \right\},$$

那么

$$|\mathcal{M}(2t+\rho, \rho)| = k_{(2t+\rho,\rho)}(n-2k-\lambda)|\mathcal{M}_1|. \tag{6.21}$$

对于

$$S = \begin{pmatrix} U & {}^tV_1 & {}^tV_2 \\ V_1 & M_{(t,\rho)} & 0 \\ V_2 & 0 & 0 \end{pmatrix} \in \mathcal{M}_1,$$

我们取

$$P = \begin{pmatrix} I & {}^tV_1 M_{(t,\rho)}^{-1} & \\ & I & \\ & & I \end{pmatrix},$$

那么 P 作用 S 就把 V_1 变成 0. 令 $\mathcal{M}_2$ 是 $\mathcal{M}_1$ 中所有形如

$$\begin{pmatrix} U & 0 & {}^tV_2 \\ 0 & M_{(t,\rho)} & 0 \\ V_1 & 0 & 0 \end{pmatrix}$$

的矩阵组成的集合. 那么

$$|\mathcal{M}_1| = q^{(2k+\lambda)(2t+\rho)}|\mathcal{M}_2|. \tag{6.22}$$

设 G_1 是 G_0 中由所有形如

$$\begin{pmatrix} R & & \\ & I & \\ & & Q \end{pmatrix}$$

的矩阵组成的子群, G_1 作用

$$S = \begin{pmatrix} U & 0 & {}^tV \\ 0 & M_{(t,\rho)} & 0 \\ V & 0 & 0 \end{pmatrix} \in \mathcal{M}_2,$$

把 V 变成 $QV\,{}^tR$. 令

$$S_{2k+\lambda,\Gamma} = \begin{pmatrix} 0 & I^{(k)} & \\ I^{(k)} & 0 & \\ & & \Gamma \end{pmatrix}, \text{这里 } \Gamma = \begin{cases} \varnothing, & \text{如果 } \lambda = 0, \\ 1, & \text{如果 } \lambda = 1, \\ \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, & \text{如果 } \lambda = 2. \end{cases} \tag{6.23}$$

由伪辛群的定义可知,$(QV\,{}^tR)S_{2k+\lambda,\Gamma}\,{}^t(QV\,{}^tR) = QVS_{2k+\lambda,\Gamma}\ {}^t(QV)$, 因而 V 在 G_1 的作用下, 它的类型不变. 设 V 关于 $S_{2k+\lambda,\Gamma}$ 是 $(m,\ 2s+\xi,\ s,\ \epsilon)$ 型矩阵, 这里 $\xi = 0,1$ 或 2, 而当 $\lambda \neq 0$ 时,$\epsilon = 0$ 或 1 分别由 $e_{2k+1} \notin V$ 或 $e_{2k+1} \in V$ 确定 (这里仍用 V 表示由 V 的行向量张成的子空间), 并且 $m,\ s,\ \xi,\ \varepsilon$ 满足如下条件:

$$\left.\begin{array}{l} \text{当 } \lambda = 0 \text{ 时}, (\xi,\varepsilon) = (0,0) \text{ 而 } 0 \leqslant 2s \leqslant m \leqslant k+s; \\ \quad \text{当 } \lambda \neq 0 \text{ 时}, (\xi,\varepsilon) = \begin{cases} (0,0),(1,0),(1,1) \text{ 或 } (2,0), & \text{如果 } \lambda = 1, \\ (0,0),(0,1),(1,0),(2,0) \text{ 或 } (2,1), & \text{如果 } \lambda = 2, \end{cases} \\ \text{并且} 0 \leqslant 2s + \max\{\xi,\varepsilon\} \leqslant m \leqslant k+s+[(\xi+\lambda-1)/2]+\varepsilon. \end{array}\right\} \tag{6.24}$$

设 $\mathcal{M}(m,\ 2s+\xi,\ \xi,\ \varepsilon;\ 2k+\lambda)$ 是 $\mathcal{M}_2$ 中块 V 关于 $M(2k+\lambda,\ \lambda,\ \Gamma)$ 是 $(m,\ 2s+\xi,\ \xi,\ \varepsilon)$ 型的所有矩阵组成的集合. 那么

$$|\mathcal{M}_2| = \sum_{m,s,\xi,\varepsilon \text{满足(6.24)}} |\mathcal{M}(m,\ 2s+\xi,\ \xi,\ \varepsilon)|. \tag{6.25}$$

现在要做的是计算 $|\mathcal{M}(m,\ 2s+\xi,\ \xi,\ \varepsilon;\ 2k+\lambda)|$. 我们需要对 $\lambda,\ \tau,\ \mu,\ \rho$ 和 ξ 的不同取值, 分别进行讨论. 这里取 $\lambda=\tau=\mu=2,\ (\rho,\ \xi,\ \varepsilon)=(0,0,1)$ 作为例子.

令

$$V=\begin{pmatrix} I & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & I & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}\begin{matrix} s \\ s \\ 1 \\ m-2s-1 \\ \sigma_1 \end{matrix}, \tag{6.26}$$
$$\begin{matrix} s & m-2s-1 & \sigma & s & m-2s-1 & \sigma & 1 & 1 \end{matrix}$$

这里 $\sigma=k-m+s+1,\ \sigma_1=n-2k-2t-m-2$.

设 $\mathcal{M}_3$ 是 $\mathcal{M}(m,\ 2s,\ 0,\ 1;\ 2k+2)$ 中所有形如

$$\begin{pmatrix} U & 0 & {}^tV \\ 0 & M_{(t,\rho)} & 0 \\ V & 0 & 0 \end{pmatrix} \tag{6.27}$$

的矩阵所成的集合, 其中 V 由 (6.26) 给定. 那么 $\mathcal{M}(m,\ 2s,\ 0,\ 1;\ 2k+2)$ 中的任一矩阵必合同于 $\mathcal{M}_3$ 中的一个矩阵. 所以

$$\begin{aligned} &|\mathcal{M}(m,\ 2s,\ 0,\ 1;\ 2k+2)| \\ =&n(n-2k-2t-2,\ m,\ 2s,\ 0,\ 1;\ 2k+2)|\mathcal{M}_3|. \end{aligned} \tag{6.28}$$

设 $\mathcal{M}_4$ 是 $\mathcal{M}_3$ 中形如 (6.27) 的矩阵组成的集合, 这里

$$U=\begin{pmatrix} U_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & U_2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & U_{33} & 0 & {}^tU_{35} & {}^tU_{36} & {}^tU_{37} & 0 \\ 0 & 0 & 0 & U_4 & 0 & 0 & 0 & 0 \\ 0 & 0 & U_{35} & 0 & U_{55} & {}^tU_{56} & {}^tU_{57} & 0 \\ 0 & 0 & U_{36} & 0 & U_{56} & U_{66} & {}^tU_{67} & 0 \\ 0 & 0 & U_{37} & 0 & U_{57} & U_{67} & U_{77} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & U_8 \end{pmatrix}, \tag{6.29}$$

而 $U_1,\ U_2,\ U_4$ 和 U_8 是对角形矩阵, 那么 $\mathcal{M}_3$ 中任一矩阵必合同于 $\mathcal{M}_4$ 中一个的矩阵. 于是

$$|\mathcal{M}_3|=q^{\frac{1}{2}m(4k-m+3)}|\mathcal{M}_4|. \tag{6.30}$$

进一步, 如果 $\mathcal{M}_3$ 中的矩阵 S 合同于 $\mathcal{M}_4$ 中的矩阵, 其中 U 由 (6.29) 给定, 那么 $S-S_2=S-M(n,2k+\lambda,\lambda)$ 合同于形如 (6.27) 的矩阵, 其中

$$U=\begin{pmatrix} U_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & U_2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & U_{33} & 0 & {}^tU_{35} & {}^tU_{36}-I & {}^tU_{37} & 0 \\ 0 & 0 & 0 & U_4 & 0 & 0 & 0 & 0 \\ 0 & 0 & U_{35} & 0 & U_{55} & {}^tU_{56} & {}^tU_{57} & 0 \\ 0 & 0 & U_{36}-I & 0 & U_{56} & U_{66} & {}^tU_{67} & 0 \\ 0 & 0 & U_{37} & 0 & U_{57} & U_{67} & U_{77} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & U_8-I \end{pmatrix}.$$

令

$$\widetilde{S}_1=0,\ \widetilde{S}_2=\begin{pmatrix} 0 & 0 & I & 0 \\ 0 & 0 & 0 & 0 \\ I & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},\ \widetilde{S}=\begin{pmatrix} U_{33} & {}^tU_{35} & {}^tU_{36} & {}^tU_{37} \\ U_{35} & U_{55} & {}^tU_{56} & {}^tU_{57} \\ U_{36} & U_{56} & U_{66} & U_{67} \\ U_{37} & U_{57} & U_{67} & U_{77} \end{pmatrix}.$$

从 $(S,S_1)\in R_{(2i+2,2)}(n)$, 可知

a) $\operatorname{rank}(\widetilde{S}-\widetilde{S}_1)=2i-2t-2m+2$.

b) 因为 $\tau=2$, 即 S 不是交错矩阵, 所以, 当 $\widetilde{S}$ 是交错矩阵时, U_1, U_2, U_4 和 U_8 不能全为零矩阵; 当 $\widetilde{S}$ 不是交错矩阵时, U_1, U_2, U_4 和 U_8 可以任意选取.

类似地, 从 $(S,\ S_2)\in R_{(2j+2,2)}(n)$ 可知

c) $\operatorname{rank}(\widetilde{S}-\widetilde{S}_2)=2j-2t-2m+2$;

d) 因为 $\mu=2$, 所以当 $\widetilde{S}$ 是交错矩阵时, U_1, U_2, U_4 和 U_8-1 不能全为零矩阵; 当 $\widetilde{S}$ 不是交错矩阵时, U_1, U_2, U_4 和 U_8-1 可以任意选取.

因此,

$$\begin{aligned}|\mathcal{M}_4|=\ &(q^m-2)p^{(2(k-m+s+1),0)}_{(2(i-t-m+1),0)(2(j-t-m+1),0)}(2k-m+2)\\&+q^mp^{(2(k-m+s+1),0)}_{(2(i-t-m+1),2)(2(j-t-m+1),2)}(2k-m+2).\end{aligned}\tag{6.31}$$

由 (6.28), (6.30) 和 (6.31) 得到

$$\begin{aligned}&|\mathcal{M}(m,2s,0,1;2k+2)|\\=\ &n(n-2k-2t-2,m,2s,0,1;2k+2)q^{\frac{1}{2}m(4k-m+3)}\{(q^m-2)\\&\qquad p^{(2(k-m+s+1),0)}_{(2(i-t-m+1),0)(2(j-t-m+1),0)}(2k-m+2)\\&+q^mp^{(2(k-m+s+1),0)}_{(2(i-t-m+1),2)(2(j-t-m+1),2)}(2k-m+2)\}.\end{aligned}$$

类似地, 对于 λ, τ, μ, ρ 和 ξ 的另外可能不同取值的情形进行讨论, 也可以得到相应

的 $|\mathcal{M}(m, 2s+\xi, \xi, \varepsilon; 2k+\lambda)|$. 我们综合这些结果成为一个统一的公式

$$\begin{aligned}&|\mathcal{M}(m,2s+\xi,\xi,\varepsilon;2k+\lambda)|\\=\ &n(n-2k-2t-\lambda-\rho,m,2s+\xi,\xi,\varepsilon;2k+\lambda)q^{\frac{1}{2}m(4k-m+2\lambda-1)}\\&\cdot\sum_{\tau_1,\mu_1}(q^m-f(\tau_1,\mu_1,\rho))p^{(2k_1+\lambda_1,\lambda_1)}_{(2i_1+\tau_1,\tau_1)(2j_1+\mu_1,\mu_1)}(2k-m+\lambda),\end{aligned}\tag{6.32}$$

这里

$$\left.\begin{aligned}&(2k_1+\lambda_1,\lambda_1)=\begin{cases}(2\sigma+1,1), & \text{如果}\,\varepsilon=0\,\text{而}\,(\lambda,\xi)\neq(2,0),\\(2\sigma+2,2), & \text{如果}\,\varepsilon=0\,\text{而}\,(\lambda,\xi)=(2,0),\\(2\sigma,0), & \text{其他情形}.\end{cases}\\&2i_1+\tau_1=2i-2t-2m+\tau-\rho,\\&2j_1+\mu_1=2j-2t-2m+\mu-\rho,\end{aligned}\right\}\tag{6.33}$$

其中, 当 $\lambda=0$ 时,$\sigma=k-m+s$; 当 $\lambda\neq0$ 时,$\sigma=k-m+s+[(\xi+\lambda-1)/2]+\varepsilon$. λ_1 依赖于 λ 和 ε; τ_1 依赖于 τ,ρ 和 λ_1; μ_1 依赖于 μ, ρ 和 λ_1. 而在 τ_1 和 μ_1 上求和则依据表 6.1 取一项, 两项, 或三项;

表 6.1　τ_1 和 μ_1 的取值

λ_1	$2i_1+\tau_1$	$2j_1+\mu_1$	(τ_1, μ_1)
0	奇	奇	(1, 1)
0	奇	偶	(1, 2)
0	偶	奇	(2, 1)
0	偶	偶	(0, 0) (2, 2)
1 或 2	奇	奇	(1, 1)
1 或 2	奇	偶	(1, 0) (1, 2)
1 或 2	偶	奇	(0, 1) (2, 1)
1 或 2	偶	偶	(0,2) (2,0) (2,2)

又

$$f(\tau_1,\mu_1,\rho)=\begin{cases}1, & \text{如果}\,\rho=0\,\text{而}\,\tau_1\,\text{和}\,\mu_1\,\text{中只有一个是}\,0,\\2, & \text{如果}\,\rho=0\,\text{而}\,\tau_1\,\text{和}\,\mu_1\,\text{都是}\,0,\\0, & \text{其他情形}.\end{cases}\tag{6.34}$$

(6.32) 式的具体推导, 可仿上面 $\lambda=\tau=\mu=2$ 的步骤进行. 这里给出推导过程中, 类似于 (6.26) 中 V 的标准形的选取及得到 (6.32) 中 $(2k_1+\lambda_1, \lambda_1)$, $(2i_1+\tau_1, \tau_1)$ 和 $(2j_1+\mu_1, \mu_1)$ 取值的简要步骤.

i) V 的选取.

设 $S_{2k+\lambda,\Gamma}$ 和 Γ 如同 (6.23) 一样地选取.

如果 $\lambda=0$, 那么 (6.26) 中的 V 取为

$$\begin{array}{c}\begin{pmatrix} I & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I & 0 & 0 \\ 0 & I & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \\ \begin{matrix} s & m-2s & \sigma & s & m-2s & \sigma \end{matrix}\end{array} \begin{matrix} s \\ s \\ m-2s \\ n-2k-2t-m \end{matrix},$$

这里 $\sigma=k-m+s$.

下面总假定 $\sigma=k+s-m+[(\xi+\lambda-1)/2]+\varepsilon$.

如果 $\lambda=1$, 由 (6.24), $(\xi,\varepsilon)=(0,0)$, $(1,0)$, $(1,1)$ 或 $(2,0)$, 那么 (6.26) 中的 V 分别取为

$$\begin{array}{c}\begin{pmatrix} I & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I & 0 & 0 & 0 \\ 0 & I & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \\ \begin{matrix} s & m-2s & \sigma & s & m-2s & \sigma & 1 \end{matrix}\end{array} \begin{matrix} s \\ s \\ m-2s \\ n-2k-2t-m-\rho-1 \end{matrix},$$

$$\begin{array}{c}\begin{pmatrix} I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \\ \begin{matrix} s & 1 & m-2s-1 & \sigma & s & 1 & m-2s-1 & \sigma & 1 \end{matrix}\end{array} \begin{matrix} s \\ s \\ 1 \\ m-2s-1 \\ n-2k-2t-m-\rho-1 \end{matrix},$$

$$\begin{array}{c}\begin{pmatrix} I & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & I & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \\ \begin{matrix} s & m-2s-1 & \sigma & s & m-2s-1 & \sigma & 1 \end{matrix}\end{array} \begin{matrix} s \\ s \\ m-2s-1 \\ n-2k-2t-m-\rho-1 \end{matrix}$$

和

$$\begin{array}{c}\begin{pmatrix} I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \\ \begin{matrix} s & 1 & m-2s-2 & \sigma & s & 1 & m-2s-2 & \sigma & 1 \end{matrix}\end{array} \begin{matrix} s \\ s \\ 1 \\ 1 \\ m-2s-2 \\ n-2k-2t-m-\rho-1 \end{matrix},$$

如果 $\lambda = 2$, 由 (6.24), $(\xi, \varepsilon) = (0,0), (0,1), (1,0), (2,0)$ 或 $(2,1)$, 那么 (6.26) 中 V 分别取为

$$\begin{array}{cc}
\begin{pmatrix}
I & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & I & 0 & 0 & 0\\
0 & I & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix} & \begin{array}{c} s\\ s\\ m-2s\\ n-2k-2t-m-\rho-2 \end{array}\\
\begin{array}{ccccccc} s & m-2s & \sigma & s & m-2s & \sigma & 2 \end{array} &
\end{array},$$

$$\begin{array}{cc}
\begin{pmatrix}
I & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & I & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1\\
0 & I & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix} & \begin{array}{c} s\\ s\\ 1\\ m-2s-1\\ n-2k-2t-m-\rho-2 \end{array}\\
\begin{array}{cccccccc} s & m-2s-1 & \sigma & s & m-2s-1 & \sigma & 1 & 1 \end{array} &
\end{array},$$

$$\begin{array}{cc}
\begin{pmatrix}
I & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & I & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\\
0 & I & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix} & \begin{array}{c} s\\ s\\ 1\\ m-2s-1\\ n-2k-2t-m-\rho-2 \end{array}\\
\begin{array}{cccccccc} s & m-2s-1 & \sigma & s & m-2s-1 & \sigma & 1 & 1 \end{array} &
\end{array},$$

$$\begin{array}{cc}
\begin{pmatrix}
I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0\\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\\
0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix} & \begin{array}{c} s\\ s\\ 1\\ 1\\ m-2s-2\\ n-2k-2t-m-\rho-2 \end{array}\\
\begin{array}{cccccccccc} s & 1 & m-2s-2 & \sigma & s & 1 & m-2s-2 & \sigma & 1 & 1 \end{array} &
\end{array},$$

$$\begin{array}{cc}
\begin{pmatrix}
I & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & I & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1\\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\\
0 & I & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & & 0 & 0
\end{pmatrix} & \begin{array}{c} s\\ s\\ 1\\ 1\\ m-2s-2\\ n-2k-2t-m-\rho-2 \end{array}\\
\begin{array}{cccccccc} s & m-2s-2 & \sigma & s & m-2s-2 & \sigma & 1 & 1 \end{array} &
\end{array}.$$

(这里 V 的选取与文献 [15] 中的 V 有点差别, 为了得到这里所对应的 V, 我们仅需改变了 [15] 中 V 的最后两行.)

ii) $(2k_1+\lambda_1,\lambda_1)$ 的取值.

我们总假定：$\lambda=0$ 时,$\sigma=k-m+s$; $\lambda\neq 0$ 时, $\sigma=k-m+s+[(\xi+\tau-1)/2]+\varepsilon$.

当 $\lambda=0$ 时,(6.27) 中的 V 只有一种选取：$(\xi,\varepsilon)=(0,0)$. 按照从 (6.26) 到 (6.31) 的步骤对 (6.27) 进行推导, 就可得到 $\widetilde{S}_2=M(2(k-m+s),2\sigma,0)$, 于是 $(2k_1+\lambda_1,\lambda_1)=(2\sigma,0)$.

当 $\lambda=1$ 时,(6.27) 中的 V 有四种选取：$(\xi,\varepsilon)=(0,0)$, $(1,0)$, $(1,1)$ 或 $(2,0)$. 如同上述的步骤进行, 就得到

$$(2k_1+\lambda_1,\ \lambda_1)=\begin{cases}(2\sigma+1,\ 1), & \text{如果 } (\xi,\ \varepsilon)=(0,\ 0),\\ (2\sigma+1,\ 1), & \text{如果 } (\xi,\ \varepsilon)=(1,\ 0),\\ (2\sigma,\ 0), & \text{如果 } (\xi,\ \varepsilon)=(1,\ 1),\\ (2\sigma+1,\ 1), & \text{如果 } (\xi,\ \varepsilon)=(2,\ 0).\end{cases}$$

当 $\lambda=2$ 时,(6.27) 中的 V 有五种选取：$(\xi,\ \varepsilon)=(0,\ 0)$, $(0,\ 1)$, $(1,0)$, $(2,0)$ 或 $(2,1)$, 同样我们可得到

$$(2k_1+\lambda_1,\ \lambda_1)=\begin{cases}(2\sigma+2,\ 2), & \text{如果 } (\xi,\ \varepsilon)=(0,\ 0),\\ (2\sigma,\ 0), & \text{如果 } (\xi,\ \varepsilon)=(0,\ 1),\\ (2\sigma+1,\ 1), & \text{如果 } (\xi,\ \varepsilon)=(1,\ 0),\\ (2\sigma+1,\ 1), & \text{如果 } (\xi,\ \varepsilon)=(2,\ 0),\\ (2\sigma,\ 0), & \text{如果 } (\xi,\ \varepsilon)=(2,1).\end{cases}$$

$(2i_1+\tau_1,\ \tau_1)$ 和 $(2j_1+\mu_1,\ \mu_1)$ 的取值, 由 $2i+\tau$, $2j+\mu$ 和 ρ 来确定.

综合前面所述的结果, 我们有

定理 6.6 设 $(\tau,\ \mu,\ \lambda)$ 取 $(0,\ 1,\ 1)$, $(0,\ 1,\ 2)$, $(0,\ 2,\ 2)$, $(1,\ 1,\ 1)$, $(1,\ 1,\ 2)$, $(1,\ 2,\ 2)$ 和 $(2,\ 2,\ 2)$, 而 ξ, ε, ρ 按照 (6.19) 和 (6.24) 所有可能的不同选取. 那么

$$\begin{aligned}p^{(2k+\lambda,\lambda)}_{(2i+\tau,\tau)(2j+\mu,\mu)}(n)=&\sum_{t,\rho\text{满足(6.19)}}k_{(2t+\rho,\rho)}(n-2k-\lambda)q^{(2k+\lambda)(2t+\rho)}\\ &\cdot\sum_{m,s,\xi,\varepsilon\text{ 满足(6.24)}}n(n-2k-2t-\lambda-\rho,m,2s+\xi,\xi,\varepsilon;2k+\lambda)q^{\frac{1}{2}m(4k-m+2\lambda-1)}\\ &\cdot\sum_{\tau_1,\mu_1}(q^m-f(\tau_1,\mu_1,\rho))p^{(2k_1+\lambda_1,\lambda_1)}_{(2i_1+\tau_1,\tau_1)(2j_1+\mu_1,\mu_1)}(2k-m+\lambda),\end{aligned}$$

其中 $(2k_1+\lambda_1)$, $(2i_1+\tau_1)$, $(2j_1+\mu_1)$ 和 $f(\tau_1,\ \mu_1,\ \rho)$ 按照 (6.33) 和 (6.34) 分别取值, 而 $(\tau_1,\ \mu_1)$ 按表 6.1 取值.

§6.6 交叉数计算续

在这一节中我们讨论满秩情形下交叉数 $p^*_{**}(n)$ 的降阶递推计算. 为了书写方便, 我们把对称矩阵的类型 $(2s+\tau,\ \tau)$ 改写如下：如果 $\tau=1$, 则记为 $2s+1$; 如果

$\tau=0$, 记为 $2s^*$; 如果 $\tau=2$, 则记为 $2(s+1)$. 对于对称矩阵 S, 用 $t(S)$ 表示 S 的类型, 例如 $t(S)=2s^*$ 指 S 是秩为 $2s$ 的交错矩阵; $t(S)=2s$ 指 S 是秩为 $2s$ 的非交错对称矩阵.

先讨论 n 为偶数的情形, 设 $n=2m$. 这时, 需要计算的是 $p_{2m^*,2m^*}^{2m^*}(2m)$, $p_{2m^*,2m}^{2m}(2m)$ 和 $p_{2m,2m}^{2m}(2m)$(注意到 $p_{2m,2m}^{2m^*}(2m)=\frac{k_{2m}(2m)}{k_{2m^*}(2m)}p_{2m^*,2m}^{2m}(2m)$). 我们已在定理 3.12 中给出 $p_{2m^*,2m^*}^{2m^*}(2m)$ 的计算方法, 为了应用方便写在这里, 不过符号有一点改变.

定理 6.7 设 $n=2m$. 我们有

$$\begin{aligned}p_{2m^*,2m^*}^{2m^*}(2m)=&\ q^{2m-2}(q^{2m-1}-q^{2m-2}-1)p_{2(m-1)^*,2(m-1)^*}^{2(m-1)^*}(2m-2)\\&+q^{2m-2}(q^{2m-2}-1)p_{2(m-1)^*,2(m-1)^*}^{2(m-2)^*}(2m-2).\end{aligned}$$

现在来计算 $p_{2m\,2m}^{2m}(2m)$. 我们给出另一种直接降阶的方法 (对比定理 4.10). 我们考虑一个 $2m$ 阶满秩非交错的对称矩阵 S 怎样从一个 $2m-1$ 阶主子矩阵 A 扩充而来? 设

$$S=\left(\begin{array}{ccc|c} & & & x_1\\ & \text{A} & & \vdots\\ & & & x_{2m-1}\\ \hline x_1 & \cdots & x_{2m-1} & x\end{array}\right),\quad t(S)=2m. \tag{6.35}$$

再设 $t(A)=(2s+\delta,\,\delta)$. 于是存在 $T\in GL_{2m-1}(\mathbb{F}_q)$ 使得

$$[T,\,1]S\,{}^t[T,\,1]=\left(\begin{array}{cccc|c}0 & I^{(s)} & & & V_1\\ I^{(s)} & 0 & & & V_2\\ & & \Delta & & V_3\\ & & & 0 & V_4\\ \hline {}^tV_1 & {}^tV_2 & {}^tV_3 & {}^tV_4 & x\end{array}\right)\begin{array}{c}s\\ s\\ \delta\\ 2m-1-2s-\delta\\ 1\end{array},$$

这里 $(x_1,\cdots,x_{2m-1})\,{}^tT=({}^tV_1\,{}^tV_2\,{}^tV_3\,{}^tV_4)=(v_1,v_2,\cdots,v_{2m-1})$. 进一步, 又合同于

$$\left(\begin{array}{cccc|c}0 & I^{(s)} & & & 0\\ I^{(s)} & 0 & & & 0\\ & & \Delta & & V_3\\ & & & 0 & V_4\\ \hline 0 & 0 & {}^tV_3 & {}^tV_4 & x\end{array}\right). \tag{6.36}$$

由于 $t(S)=2m$, 所以 $\operatorname{rank}A=2m-1$ 或 $\operatorname{rank}A=2m-2$.

(a) 如果 $\operatorname{rank} A = 2m-1$, 那么 $s = m-1, \Delta = 1, V_4 = \varnothing$(不出现), 这时 $V_3 = v_{2m-1}$, 矩阵 (6.36) 进一步合同于

$$\left(\begin{array}{ccc|c} 0 & I^{(m-1)} & & 0 \\ I^{(m-1)} & 0 & & 0 \\ & & 1 & 0 \\ \hline 0 & 0 & 0 & x' \end{array}\right),$$

这里 $x' = x + v_{2m-1}^2 \neq 0$. 于是可知, 如果 $\operatorname{rank} A = 2m-1$, 那么对 A 添加 1 行 1 列可使得到的 S 有 $t(S) = 2m$. 由于 V_1, V_2 不影响 S 的秩, 可以任意选取, 而 $x \neq v_{2m-1}^2$, 所以这样的 S 可得到 $q^{2m-1}(q-1)$ 个.

(b) 设 $t(A) = 2(m-1)^*$, 那么 $s = m-1, \Delta = \varnothing(V_3$ 不出现$), V_4 = v_{2m-1} \neq 0, x \neq 0$. 这时可得到 $q^{2m-2}(q-1)^2$ 个 S 使 $t(S) = 2m$.

(c) 设 $t(A) = 2(m-1)$, 那么 $s = m-2$, $\Delta = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, ${}^tV_3 = (v_{2m-3}\ v_{2m-2})$, $V_4 = v_{2m-1}$. 这时矩阵 (6.36) 进一步合同于

$$\left(\begin{array}{ccccc|c} 0 & I^{(m-2)} & & & & 0 \\ I^{(m-2)} & 0 & & & & 0 \\ & & 0 & 1 & & 0 \\ & & 1 & 1 & & 0 \\ & & & & 0 & v_{2m-1} \\ \hline 0 & 0 & 0 & 0 & v_{2m-1} & x' \end{array}\right),$$

这里 $v_{2m-1} \neq 0$, $x' = x + v_{2m-3}^2$. 这样可得 $q^{2m-1}(q-1)$ 个 S 使 $t(S) = 2m$.

还应指出, 每个 $t(S) = 2m$ 的 $2m$ 阶对称矩阵 S 都可从其左上角 $2m-1$ 阶主子矩阵如上扩充而得到.

现在, 令

$$H = \begin{pmatrix} I^{(2m-1)} & U \\ {}^tU & \omega \end{pmatrix}, \tag{6.37}$$

这里 ${}^tU = (y_1, \cdots, y_{2m-1})$, $y_i \in \mathbb{F}_q$. 再令 $\mathcal{M}$ 为如下 $2m$ 阶对称矩阵对子组成的集合

$$\mathcal{M} = \{(H, S) | t(S) = 2m, t(S+H) = 2m\}.$$

我们用两种方法来计算 $|\mathcal{M}|$.

第一种方法是先取 H 然后取 S. 当 $\omega \neq {}^tUU$ 时, $t(H) = 2m$. 这时 S 有

$p_{2m\,2m}^{2m}(2m)$ 个选取, 这种对子 (H, S) 有 $q^{2m-1}(q-1)\cdot p_{2m\,2m}^{2m}(2m)$ 个. 当 $\omega = {}^tUU$ 时 $t(H) = 2m-1$; 这时 S 有 $p_{2m\,2m}^{2m-1}(2m)$ 个选取, 这种对子 (H, S) 的个数为 $q^{2m-1}\cdot p_{2m\,2m}^{2m-1}(2m)$. 因此

$$|\mathcal{M}| = q^{2m-1}(q-1)\cdot p_{2m\,2m}^{2m}(2m) + q^{2m-1}\cdot p_{2m\,2m}^{2m-1}(2m). \tag{6.38}$$

第二种方法是先取 S 然后取 H. 考虑 S 有形状 (6.35). 由于要求 $t(S) = 2m$, 它的左上角 $2m-1$ 阶主子矩阵 A 有 $t(A) = 2m-1$ 或 $2(m-1)^*$ 或 $2(m-1)$. 又由于要求 $t(S+H) = 2m$, 所以 $S+H$ 的主子矩阵 $A+I^{(2m-1)}$ 也有 $t(A+I^{(2m-1)}) = 2m-1$ 或 $2(m-1)^*$ 或 $2(m-1)$. 这样,A 就有 9 种可能情形.

(1) $t(A) = 2m-1$ 而 $t(A+I^{(2m-1)}) = 2m-1$. 这样 A 有 $p_{2m-1\,2m-1}^{2m-1}(2m-1)$ 个. 取定一个这样的 A 后, 将它扩充成 S 使 $t(S) = 2m$. 由 (a) 可知, 这种 S 可有 $q^{2m-1}(q-1)$ 个. 取定这样一个 S, 设添加上的最后一行为 $(x_1, \cdots, x_{2m-1}, x)$. 然后, 将 $A+I^{(2m-1)}$ 扩充成 $2m$ 阶对称矩阵 Y 使 $t(Y) = 2m$. 同样由 (a) 知这样的 Y 有 $q^{2m-1}(q-1)$ 个. 取定一个 Y, 设添加上的最后一行为 $(z_1, \cdots, z_{2m-1}, z)$. 令 $y_i = x_i + z_i\,(i = 1, \cdots, 2m-1)$, $\omega = x+z$. 并令 H 为 $I^{(2m-1)}$ 如 (6.37) 添加 $y_1, \cdots, y_{2m-1}, \omega$ 所得者, 那么 $Y = S+H$, $t(S+H) = 2m$, $(H, S) \in \mathcal{M}$. 因此, 在这种情形可得对子 (H, S) 的个数为 $q^{2m-1}(q-1)\cdot q^{2m-1}(q-1)\cdot p_{2m-1\,2m-1}^{2m-1}(2m-1)$.

(2) $t(A) = 2m-1$ 而 $t(A+I) = 2(m-1)^*$. 类似地讨论可知, 在这种情形可得对子 (H, S) 的个数为 $q^{2m-1}(q-1)\cdot q^{2m-2}(q-1)^2\cdot p_{2m-1\,2(m-1)^*}^{2m-1}(2m-1)$.

(3) $t(A) = 2m-1$ 而 $t(A+I) = 2(m-1)$.这时可得对子 (H, S) 的个数为 $q^{2m-1}(q-1)\cdot q^{2m-1}(q-1)\cdot p_{2m-1\,2(m-1)}^{2m-1}(2m-1)$.

(4) $t(A) = 2(m-1)^*$ 而 $t(A+I) = 2m-1$.这时可得对子 (H, S) 的个数为 $q^{2m-2}(q-1)^2\cdot q^{2m-1}(q-1)\cdot p_{2(m-1)^*\,2m-1}^{2m-1}(2m-1)$.

(5) $t(A) = 2(m-1)^*$ 而 $t(A+I) = 2(m-1)^*$. 这时 (H, S) 的个数为 0.

(6) $t(A) = 2(m-1)^*$ 而 $t(A+I) = 2(m-1)$. 这时可得对子 (H, S) 的个数为 $q^{2m-2}(q-1)^2\cdot q^{2m-1}(q-1)\cdot p_{2(m-1)^*\,2(m-1)}^{2m-1}(2m-1)$.

(7) $t(A) = 2(m-1)$ 而 $t(A+I) = 2m-1$. 这时可得对子 (H, S) 的个数为 $q^{2m-1}(q-1)\cdot q^{2m-1}(q-1)\cdot p_{2(m-1)\,2m-1}^{2m-1}(2m-1)$.

(8) $t(A) = 2(m-1)$ 而 $t(A+I) = 2(m-1)^*$. 这时可得对子 (H, S) 的个数为 $q^{2m-1}(q-1)\cdot q^{2m-2}(q-1)^2\cdot p_{2(m-1)\,2(m-1)^*}^{2m-1}(2m-1)$.

(9) $t(A) = 2(m-1)$ 而 $t(A+I) = 2(m-1)$. 这时可得对子 (H, S) 的个数为 $q^{2m-1}(q-1)\cdot q^{2m-1}(q-1)\cdot p_{2(m-1)\,2(m-1)}^{2m-1}(2m-1)$.

综合 (1) ~ (9), 按第二种方法计算, 可得

$$
\begin{aligned}
|\mathcal{M}| = & q^{4m-2}(q-1)^2 \cdot p^{2m-1}_{2m-1\,2m-1}(2m-1) \\
& + 2q^{4m-3}(q-1)^3 \cdot p^{2m-1}_{2m-1\,2(m-1)^*}(2m-1) \\
& + 2q^{4m-2}(q-1)^2 \cdot p^{2m-1}_{2m-1\,2(m-1)}(2m-1) \\
& + 2q^{4m-3}(q-1)^3 \cdot p^{2m-1}_{2(m-1)\,2(m-1)^*}(2m-1) \\
& + q^{4m-2}(q-1)^2 \cdot p^{2m-1}_{2(m-1)\,2(m-1)}(2m-1).
\end{aligned} \tag{6.39}
$$

由 (6.38) 和 (6.39), 我们得到下面的计算公式

定理 6.8 在 $n=2m$ 时, 我们有

$$
\begin{aligned}
p^{2m}_{2m\,2m}(2m) = & q^{2m-1}(q-1)p^{2m-1}_{2m-1\,2m-1}(2m-1) \\
& + 2q^{2m-2}(q-1)^2 p^{2m-1}_{2m-1\,2(m-1)^*}(2m-1) \\
& + 2q^{2m-1}(q-1)p^{2m-1}_{2m-1\,2(m-1)}(2m-1) \\
& + 2q^{2m-2}(q-1)^2 p^{2m-1}_{2(m-1)\,2(m-1)^*}(2m-1) \\
& + q^{2m-1}(q-1)p^{2m-1}_{2(m-1)\,2(m-1)}(2m-1) - \frac{1}{q-1}p^{2m-1}_{2m\,2m}(2m).
\end{aligned}
$$

如果我们在上面的讨论中要求 S 有 $t(S)=2m^*$, 那么就可得到 $p^{2m}_{2m^*\,2m}(2m)$ 的计算公式. 这时设 S 有形状 (6.1) 而 $t(S)=2m^*$, 那么其左上角矩阵 A 必有 $t(A)=2(m-1)^*$, 而每个这样的 A 可扩充成 $q^{2m-2}(q-1)$ 个 $2m$ 阶满秩交错矩阵. 注意到 $A+I^{2m-1}$ 恒为非交错的, 所以 $t(A+I^{(2m-1)})=2(m-1)$ 或 $t(A+I^{(2m-1)})=2m-1$. 仿照上面的讨论我们就得到

定理 6.9 设 $n=2m$. 那么

$$
\begin{aligned}
p^{2m}_{2m^*\,2m}(2m) = & q^{2m-2}(q-1)p^{2m-1}_{2(m-1)^*\,2(m-1)}(2m-1) \\
& + q^{2m-2}(q-1)p^{2m-1}_{2(m-1)^*\,2m-1}(2m-1) - \frac{1}{q-1}p^{2m-1}_{2m^*\,2m}(2m).
\end{aligned}
$$

最后讨论 n 为奇数的情形, 设 $n=2m+1$. 我们仍需用这种办法来计算 $p^{2m+1}_{2m+1\,2m+1}(2m+1)$. 设

$$
S = \left(\begin{array}{ccc|c} & & & x_1 \\ & A & & \vdots \\ & & & x_{2m} \\ \hline x_1 & \cdots & x_{2m} & x \end{array}\right), \quad t(S) = 2m+1.
$$

再设 $t(A)=(2s+\delta,\,\delta)$. 于是存在 $T\in GL_{2m}(\mathbb{F}_q)$ 使得

$$[T,\,1]S\,{}^t[T,\,1]=\left(\begin{array}{cccc|c} 0 & I^{(s)} & & & V_1\\ I^{(s)} & 0 & & & V_2\\ & & \Delta & & V_3\\ & & & 0 & V_4\\ \hline {}^tV_1 & {}^tV_2 & {}^tV_3 & {}^tV_4 & x\end{array}\right)\begin{array}{c} s\\ s\\ \delta\\ 2m-2s-\delta\\ 1\end{array},$$

这里 $(x_1,\cdots,x_{2m})\,{}^tT=({}^tV_1\,{}^tV_2\,{}^tV_3\,{}^tV_4)=(v_1,\cdots,v_{2m})$. 进一步又可合同于

$$\left(\begin{array}{cccc|c} 0 & I^{(s)} & & & 0\\ I^{(s)} & 0 & & & 0\\ & & \Delta & & V_3\\ & & & 0 & V_4\\ \hline 0 & 0 & {}^tV_3 & {}^tV_4 & x\end{array}\right).$$

由于 $t(S)=2m+1$, 所以 $\operatorname{rank}A=2m-1$, 或 $t(A)=2m^*$, 或 $t(A)=2m$.

(a) 如果 $\operatorname{rank}A=2m-1$, 那么 $s=m-1$, $\Delta=1$, $V_3=v_{2m-1}$, $V_4=v_{2m}\neq 0$. 这时可进一步合同于

$$\left(\begin{array}{cccc|c} 0 & I^{(m-1)} & & & 0\\ I^{(m-1)} & 0 & & & 0\\ & & 1 & & 0\\ & & & 0 & v_{2m}\\ \hline 0 & 0 & 0 & v_{2m} & x'\end{array}\right),$$

这里 $x'=x+v_{2m-1}^2$. 于是可知, 由 $\operatorname{rank}A=2m-1$, 那么对 A 添加 1 行 1 列可使得到的 S 有 $t(S)=2m+1$. 由于 V_1, V_2, v_{2m-1} 和 x 不影响 S 的秩, 可以任意选取, 所以这样的 S 可得到 $q^{2m}(q-1)$ 个.

(b) 设 $t(A)=2m^*$, 那么 $s=m$, $\Delta=\varnothing$(V_3 不出现), V_4 不出现.$x\neq 0$. 这时可得到 $q^{2m}(q-1)$ 个 S 使 $t(S)=2m+1$.

(c) 设 $t(A)=2m$, 那么 $s=m-1$, $\Delta=\begin{pmatrix}0&1\\1&1\end{pmatrix}$, V_4 不出现,${}^tV_3=(v_{2m-1},\,v_{2m})$. 这时可进一步合同于

$$\left(\begin{array}{cccc|c} 0 & I^{(m-1)} & & & 0\\ I^{(m-1)} & 0 & & & 0\\ & & 0 & 1 & 0\\ & & 1 & 1 & 0\\ \hline 0 & 0 & 0 & 0 & x'\end{array}\right),$$

这里 $x' = x + v_{2m-1}^2 \neq 0$. 这样可得到 $q^{2m}(q-1)$ 个 S 使 $\mathrm{rank}\, S = 2m+1$.

现在, 令

$$H = \left(\begin{array}{c|c} I^{(2m)} & U \\ \hline {}^tU & \omega \end{array}\right),$$

这里 ${}^tU = (y_1, \cdots, y_{2m})$, $y_i \in \mathbb{F}_q$. 再令 $\mathcal{M}$ 为如下 $2m+1$ 阶对称矩阵对子作成的集合

$$\mathcal{M} = \{(H, S) | \mathrm{rank}\, S = 2m+1,\ \mathrm{rank}\,(S+H) = 2m+1\}.$$

我们可用两种方法来计算 $|\mathcal{M}|$.

第一种方法是先取 H 然后取 S. 当 $\omega \neq {}^tUU$ 时, $\mathrm{rank}\, H = 2m+1$. 这时, S 有 $p_{2m+1\, 2m+1}^{2m+1}(2m+1)$ 个选取, 这样的对子 (H, S) 的个数为 $q^{2m}(q-1) \cdot p_{2m+1\, 2m+1}^{2m+1}(2m+1)$. 当 $\omega = {}^tUU$ 时, $t(H) = 2m$; 这时 S 有 $p_{2m+1\, 2m+1}^{2m}(2m+1)$ 个选取, 这样的对子 (H, S) 的个数为 $q^{2m} \cdot p_{2m+1\, 2m+1}^{2m}(2m+1)$. 因此

$$|\mathcal{M}| = q^{2m}(q-1) \cdot p_{2m+1\, 2m+1}^{2m+1}(2m+1) + q^{2m} \cdot p_{2m+1\, 2m+1}^{2m}(2m+1).$$

第二种方法是先取 S 然后取 H. 由于要求 $\mathrm{rank}\, S = 2m+1$, 它的左上角 $2m$ 阶子矩阵 A 有 $\mathrm{rank}\, A = 2m-1$ 或 $t(A) = 2m^*$ 或 $t(A) = 2m$. 另一方面, 要 $\mathrm{rank}\,(S+H) = 2m+1$, 所以 $S+H$ 的左上角 $2m$ 阶子矩阵 $A+I$ 有 $\mathrm{rank}\,(A+I) = 2m-1$, 或 $t(A+I) = 2m^*$, 或 $t(A+I) = 2m$. 这样, A 就有 9 种可能的选取. 由 (a), (b) 和 (c) 可知,

按第二种方法计算可得

$$\begin{aligned} |\mathcal{M} = |q^{4m}(q-1)^2\{&p_{2m-1\, 2m-1}^{2m}(2m) + 2p_{2m-1\, 2m^*}^{2m}(2m) \\ &+ 2p_{2m-1\, 2m}^{2m}(2m) + 2p_{2m\, 2m^*}^{2m}(2m) + p_{2m\, 2m}^{2m}(2m)\}. \end{aligned}$$

这样, 我们有下面的

定理 6.10 在 $n = 2m+1$ 时, 有

$$\begin{aligned} p_{2m+1\, 2m+1}^{2m+1}(2m+1) = q^{2m}(q-1)\{&p_{2m-1\, 2m-1}^{2m}(2m) + 2p_{2m-1,\, 2m^*}^{2m}(2m) \\ &+ 2p_{2m-1\, 2m}^{2m}(2m) + 2p_{2m,\, 2m^*}^{2m}(2m) \\ &+ p_{2m,\, 2m}^{2m}(2m)\} - \frac{1}{q-1} p_{2m+1,\, 2m+1}^{2m}(2m+1). \end{aligned}$$

§6.7 q 为偶数时 $\mathrm{Sym}(n, q)$ 的一个聚合方案

在这一节中, 我们仿照 §5.7 来讨论当 q 为偶数时 $\mathrm{Sym}(n, q)$ 的一个聚合方案. 应该指出, 这个结合方案并不是 q 为偶数时的 $\mathrm{Quad}\,(n, q)$.

设 $\mathbb{F}_q$ 为特征数为 2 的有限域, $\mathrm{Sym}(n, q)$ 为 $\mathbb{F}_q$ 上 $n\times n$ 对称矩阵的结合方案, $R_{(2s+\tau,\tau)}$ 为它的结合类, 等等. 令

$$\overline{R}_i=\{(X, Y)|X, Y\in S(n, q), \mathrm{rank}(Y-X)=2i-1 \text{ 或 } 2i\}, 0\leqslant i\leqslant\left[\frac{n+1}{2}\right]. \tag{6.40}$$

我们有

定理 6.11　设 $\mathbb{F}_q$ 为特征数为 2 的有限域,S(n, q) 上如 (6.40) 定义结合类, 作成一个类数为 $[\frac{n+1}{2}]$ 的 P 多项式方案, 记作 $\overline{\mathrm{Sym}}(n, q)$, 它的参数与 $\mathrm{Alt}\,(n+1, q)$ 的参数一致.

和定理 5.18 的证明一样, 我们只需要证明下面的

引理 6.12　对于 $i, j\in\{0, 1, \cdots, [\frac{n+1}{2}]\}$,

$$p_{1i}^j:=|\{S\in S(n, q)|(S_1, S)\in\overline{R}_1, (S, S_2)\in\overline{R}_i\}|$$

为常数, 只要 $(S_1, S_2)\in\overline{R}_j$. 这里,

(i) $p_{1i}^i=0$, 如果 $|i-j|=0$.

(ii) $p_{1i}^{i-1}=\frac{q^{2i-2}(q^{2i}-1)}{q^2-1}$.

(iii) $p_{1\,i}^i=\frac{(q^{2i}-1)(q^{n+1}+q^n-q^{2i}-q^{2i-2}-1)}{q^2-1}$.　　(6.41)

(iv) $p_{1i}^{i+1}=\frac{q^{4i}(q^{n-2i}-1)(q^{n-2i+1}-1)}{q^2-1}$.

证明　不失一般性, 可设 $S_1=0$. 而 $S_2=M(n, 2i-1, 1)$, $M(n, 2i, 0)$ 和 $M(n, 2i, 2)$. 令

$$d_{h,l}(S_2)=|\{S\in S(n, q)|\mathrm{rank}\,S=l, \mathrm{rank}\,(S-S_2)=h\}|.$$

对于 $l\in\{1, 2\}$, $h\in\{2i-3, 2i-2, 2i+1, 2i+2\}$ 和 $\tau\in\{0, 2\}$. 我们算出了 $d_{h,l}(S_2)$ 的值, 并把它们列成下面表 6.2 和表 6.3.

表 6.2　$S_2=M(n, 2i-1, 1)$ 时的取值

h	$l=2$	$l=1$
$2i-3$	$\frac{q^{2i-2}(q^{2i-2}-1)}{q^2-1}$	0
$2i-2$	$q^{2i-2}(q^{2i-2}-1)$	q^{2i-2}
$2i+1$	$\frac{q^{4i}(q^{n-2i}-1)(q^{n-2i+1}-1)}{q^2-1}$	0
$2i+2$	0	0

表 6.3 $S_2=M(n, 2i, \tau)$ 时的取值

h	$l=2$	$l=1$
$2i-3$	0	0
$2i-2$	$\dfrac{q^{2i-2}(q^{2i}-1)}{q^2-1}$	0
$2i+1$	$q^{2i}(q^{n-2i}-1)(q^{2i}-1)$	$q^{2i}(q^{n-2i}-1)$
$2i+2$	$\dfrac{q^{4i+2}(q^{n-2i}-1)(q^{n-2i-1}-1)}{q^2-1}$	0

表 6.3 中的数值仅与 S_2 的秩有关而与 τ 无关, 虽然在计算中涉及到 τ.

容易看出 (i) 是成立的. $p^i_{1\,i-1}$ 和 $p^i_{1\,i+1}$ 可以从上面的表中所列数值得知它们的常数. 至于 $p^i_{1\,i}$ 可从下面的关系式中导出.

$$\begin{aligned} p^i_{1\,i-1}+p^i_{1\,i}+p^i_{1\,i+1} &= |\{S\in S(n, q)|\mathrm{rank}\, S=1 \text{ 或 } 2\}| \\ &= k_{(1,1)}(n)+k_{(2,0)}(n)+k_{(2,2)}(n) \\ &= \frac{(q^{n+1}-1)(q^n-1)}{q^2-1}. \end{aligned}$$

现在, 我们以 $d_{2i-2,2}(S_2)$, $S_2=M(n, 2i, 0)$ 为例说明如何计算上面表中各个数值. 首先注意到

$$d_{2i-2,2}(S_2)=p^{(2i,0)}_{(2,0)(2i-2,0)}(n)+p^{(2i,0)}_{(2,2)(2i-2,2)}(n). \tag{6.42}$$

为了方便, 我们利用关系式

$$\begin{aligned} p^{(2i,0)}_{(2,0)(2i-2,0)}(n) &= \frac{k_{(2,0)}(n)}{k_{(2i,0)}(n)}p^{(2,0)}_{(2i-2,0)(2i,0)}(n), \\ p^{(2i,0)}_{(2,2)(2i-2,2)}(n) &= \frac{k_{(2,2)}(n)}{k_{(2i,2)}(n)}p^{(2,2)}_{(2i-2,2)(2i,0)}(n) \end{aligned} \tag{6.43}$$

改为计算 $p^{(2,0)}_{(2i-2,0)(2i,0)}(n)$ 和 $p^{(2,2)}_{(2i-2,2)(2i,0)}(n)$.

先计算 $p^{(2,0)}_{(2i-2,0)(2i,0)}(n)$. 令

$$S_1=0,\ \ S_2=\begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & 0^{n-2)} \end{pmatrix}.$$

再令

$$\mathcal{M}=\{S\in S(n, q)|S\sim M(n, 2i-2, 0),\ S-S_2\sim M(n, 2i, 0)\}.$$

设 $S \in \mathcal{M}$. 将 S 按 S_2 分块,$S = \begin{pmatrix} U & V \\ {}^tV & W \end{pmatrix}$. 由于 S 为交错矩阵, 所以 W 必为交错的. 设 $\operatorname{rank} W = 2t$, 那么, 存在合同变换使 S_1, S_2 不动, 而将 S 化为

$$\begin{pmatrix} U & 0 & {}^tV \\ 0 & K_t & 0 \\ V & 0 & 0 \end{pmatrix} \begin{matrix} 2 \\ 2t \\ n-2t-2 \end{matrix}. \tag{6.44}$$

令 $\mathcal{M}_t$ 为 $\mathcal{M}$ 中形如 (6.44) 的矩阵所成集合, 那么, 我们有

$$|\mathcal{M}| = \sum_t k_{(2t,\,0)}(n-2) \cdot q^{4t}|\mathcal{M}|_t. \tag{6.45}$$

设 $S \in \mathcal{M}_t$, 现在, 分别对 $V = 0$ 和 $V \neq 0$ 两种情形讨论之.

(a) $V = 0$.

如果 $U = 0$, 那么 $t = i-1, S - S_2 \sim M(n,\, 2i,\, 0)$. 这时 $|\mathcal{M}_{t-1}| = 1$. 如果 $U \neq 0$, 那么 $U = \begin{pmatrix} 0 & b \\ b & 0 \end{pmatrix}, b \neq 0$. 于是 $t = i-2$, 而 $\operatorname{rank}(S - S_2) \leqslant 2i-2$. 这种情形不可能发生.

(b) $V \neq 0$.

如果 $\operatorname{rank} V = 1$, 那么存在合同变换使 S_1, S_2 均不动, 而将形如 (6.44) 的 S 的右上角 V 化为 $\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \end{pmatrix}$. 由于 $\operatorname{rank} S = 2i-2$, 有 $t = i-2$, 且对任意 $U = \begin{pmatrix} 0 & b \\ b & 0 \end{pmatrix}$ 均有 $S - S_2 \sim M(n,\, 2i-2,\, 0)$. 这种情形不可能发生.

如果 $\operatorname{rank} V = 2$, 那么存在合同变换使 S_1, S_2 均不动, 而将 S 中的 V 化为 $\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \end{pmatrix}$. 这时 $t = i-3$, 而对于任意 U 均有 $S - S_2 \sim M(n,\, 2i-2,\, 0)$. 这种情形也不可能发生.

由上面的讨论可知,

$$p^{(2,\,0)}_{(2i-2,\,0)(2i,\,0)}(n) = k_{(2i-2,\,0)}(n-2) \cdot q^{4i-4} = \frac{q^{(i-1)(i+2)} \displaystyle\prod_{j=n-2i+1}^{n-2} (q^j - 1)}{\displaystyle\prod_{j=1}^{i-1} (q^{2i} - 1)}. \tag{6.46}$$

同样的办法, 我们计算得

$$p^{(2,\,2)}_{(2i-2,\,0)(2i,\,2)}(n) = 0. \tag{6.47}$$

由 (6.42), (6.43), (6.46) 和 (6.47), 我们得到

$$d_{2i-2,\,2}(S_2) = \frac{q^{2i-2}(q^{2i} - 1)}{q^2 - 1}.$$

这就是我所计算的表 6.3 中的那个值. □

从定理 5.15 我们知道, 在 q 为奇数时, 尽管 $\mathrm{Sym}(n,q)$ 的聚合方案 $\mathrm{Quad}(n,q)$ 与 $\mathrm{Alt}(n+1,q)$ 有相同的参数, 但 $\mathrm{Quad}(n, q)$ 并不与 $\mathrm{Alt}(n+1, q)$ 同构. 然而在 q 为偶数时, $\mathrm{Sym}(n, q)$ 的聚合方案 $\overline{\mathrm{Sym}}(n, q)$ 不仅与 $\mathrm{Alt}(n+1, q)$ 有相同的参数, 而且 $\overline{\mathrm{Sym}}(n, q)$ 与 $\mathrm{Alt}(n+1, q)$ 同构 ([11], [16]). 我们证明下面的

定理 6.13 设 q 为 2 的方幂. $\mathrm{Sym}(n, q)$ 的聚合方案 $\overline{\mathrm{Sym}}(n, q)$ 与 $\mathrm{Alt}(n+1, q)$ 同构.

证明 对于 $\mathbb{F}_q$ 上任一 $(n+1)\times(n+1)$ 交错矩阵 A 写成形式 $A = \begin{pmatrix} 0 & \mathbf{a} \\ {}^t\mathbf{a} & A_0 \end{pmatrix}$. 令 ψ 为 $\mathbb{F}_q$ 上 $(n+1)\times(n+1)$ 交错矩阵的集合 $\mathcal{K}(n+1, q)$ 到 $S(n, q)$ 的映射:

$$\psi(A) = A_0 + {}^t\mathbf{a}\mathbf{a}.$$

易见, ψ 是一一的.

现在, 我们证明上述映射保持结合关系. 由于 $\mathrm{Alt}(n+1, q)$ 和 $\overline{\mathrm{Sym}}(n, q)$ 分别关于它们的结合关系之顺序 $R_1, \cdots, R_{[\frac{n+1}{2}]}$ 及 $\bar{R}_1, \cdots, \bar{R}_{[\frac{n+1}{2}]}$ 是 P 多项式的, 我们只需证明映射 $\psi(R_1) = \bar{R}_1$ 即可. 设 $A, B \in \mathcal{K}(n+1, q)$, 写

$$A = \begin{pmatrix} 0 & \mathbf{a} \\ {}^t\mathbf{a} & A_0 \end{pmatrix}, \ B = \begin{pmatrix} 0 & \mathbf{b} \\ {}^t\mathbf{b} & B_0 \end{pmatrix}.$$

设 $(A, B) \in R_1$, 即 $\mathrm{rank}\,(A+B) = 2$. 往证 $(\psi(A), \psi(B)) \in \bar{R}_1$, 即

$$\mathrm{rank}(A_0 + B_0 + {}^t\mathbf{a}\mathbf{a} + {}^t\mathbf{b}\mathbf{b}) = 1 \text{ 或 } 2 \tag{6.48}$$

注意到

$$\mathrm{rank}\begin{pmatrix} 0 & \mathbf{a}+\mathbf{b} \\ {}^t\mathbf{a} + {}^t\mathbf{b} & A_0 + B_0 \end{pmatrix} = 2,$$

我们区别下面两种情形讨论之.

(a) $A_0 + B_0 = 0$. 这时 $\mathbf{a}+\mathbf{b} \neq 0$, 那么显然 (6.48) 成立.

(b) $A_0 + B_0 \neq 0$. 那么 $\mathrm{rank}\,(A_0 + B_0) = 2$. 于是存在 $P_1 \in GL_n\,(\mathbb{F}_q)$ 使得

$${}^tP_1(A_0 + B_0)P_1 = \begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & 0^{(n-2)} \end{pmatrix}.$$

由 $\mathrm{rank}\,(A+B) = 2$, 我们有

$${}^t\begin{pmatrix} 1 & \\ & P_1 \end{pmatrix}\begin{pmatrix} 0 & \mathbf{a}+\mathbf{b} \\ {}^t\mathbf{a} + {}^t\mathbf{b} & A_0 + B_0 \end{pmatrix}\begin{pmatrix} 1 & \\ & P_1 \end{pmatrix} = \begin{pmatrix} 0 & c_1 & c_2 & \\ c_1 & 0 & 1 & \\ c_2 & 1 & 0 & \\ & & & 0^{(n-2)} \end{pmatrix},$$

这里 $(c_1, c_2, 0, \cdots, 0) = (\mathbf{a}+\mathbf{b})P_1$. 存在 $P_2 \in Sp_2(\mathbb{F}_q)$ 使得 $(c_1, c_2)P_2 = (\varepsilon, 0)$, $\varepsilon = 0$ 或 1. 令 $P = P_1 \begin{pmatrix} P_2 & \\ & I^{(n-2)} \end{pmatrix}$, 那么

$$^tP(A_0 + B_0)P = \begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & 0^{(n-2)} \end{pmatrix} \text{ 及 } (\mathbf{a}+\mathbf{b})P = (\varepsilon, 0, \cdots, 0).$$

设 $\mathbf{a}P = (a_1, \cdots, a_n)$, 那么 $\mathbf{b}P = (\varepsilon + a_1, a_2, \cdots, a_n)$. 这样,

$$^tP(A_0 + B_0 + {}^t\mathbf{aa} + {}^t\mathbf{bb})P = \begin{pmatrix} \varepsilon & 1+\varepsilon a_2 & \varepsilon a_3 & \cdots & \varepsilon a_n \\ 1+\varepsilon a_2 & & & & \\ \varepsilon a_3 & & 0 & & \\ \vdots & & & & \\ \varepsilon a_n & & & & \end{pmatrix},$$

它的秩为 1 或 2. 于是 (6.48) 成立. □

§6.8 Sym(n, q) 的自同构

关于特征数为 2 的 $\mathbb{F}_q$ 上对称矩阵结合方案的自同构, 我们有下面的

定理 6.14 设 $n \geqslant 2$. 那么

(i) Sym(n, q) 的内自同构有如下形状

$$S \longrightarrow {}^tPSP + S_0, \forall S \in S(n, q), S_0 \in S(n, q). \tag{6.49}$$

(ii) Inn Sym(n, q) =Aut Sym(n, q).

证明 (i) 设 f 是 Sym(n, q) 的一个内自同构. 由定义 (见 §1.9), f 使每个关系 $R_{(2s+\tau,\tau)}$ 不变, 也就是说, f 保持 $S(n, q)$ 中任一对矩阵之差的类型不变, 特别地, 对于 $A, B \in S(n, q)$, 而 rank $(B - A) = 1$, 则 rank $(f(B) - f(A)) = 1$. 由对称矩阵几何基本定理 (见 [16]), 可知 f 具有形状

$$f(X) = a\,{}^tP\,{}^\sigma XP + S_0, \forall X \in S(n, q), \tag{6.50}$$

这里 $a \in \mathbb{F}_q^*$, $P \in GL_n(\mathbb{F}_q)$, σ 是域 $\mathbb{F}_q$ 的一个自同构, $S_0 \in S(n, q)$. 由 $\mathbb{F}_q$ 的特征数为 2 可知 $\mathbb{F}_q^2 = \mathbb{F}_q$, 因而 $a^{\frac{1}{2}} \in \mathbb{F}_q$.

我们用 $a^{\frac{1}{2}}P$ 代替 P, 可以去掉 (6.50) 等号右边的 a. 注意到 [16] 中额外 (extra) 类型的双射在这里不出现, 因此 (6.49) 成立.

(ii) 对于任意 $f \in$ Aut Sym(n, q), 设

$$f : R_{(2i+\tau,\tau)} \longrightarrow R_{(2i+\tau,\tau)^{\sigma(f)}},$$

这里 $\sigma(f)$ 是由 f 在 $\{(2i+\tau,\tau)|1\leqslant 2i+\tau\leqslant n,\ \tau=0,\ 1$ 或 $2\}$ 上导出的一个置换. 由定理 1.27, 有

$$p^{(2k+\lambda,\lambda)}_{(2i+\tau,\tau),(2j+\mu,\mu)}(n)=p^{(2k+\lambda,\lambda)^{f(\sigma)}}_{(2i+\tau,\tau)^{f(\sigma)}(2j+\mu,\mu)^{f(\sigma)}}(n).$$

特别地,

$$k_{(2i+\tau,\tau)}(n)=k_{(2i+\tau,\tau)^{\sigma(f)}}(n),$$

这里 Sym(n, q) 的结合类 $R_{(2i+\tau,\tau)}(n)$ 的价

$$k_{(2\nu+\tau,\tau)}(n)=q^{i(i\pm1)}\frac{\prod\limits_{j=n-2i-\tau+1}^{n}(q^j-1)}{\prod\limits_{j=1}^{i}(q^{2j}-1)},\tag{6.51}$$

其中, 当 $\tau=0$ 时, 取“$-$”; 当 $\tau\neq0$ 时, 取“$+$”. 容易证明 (6.51) 对于不同的 $(2i+\tau,\tau)$ 和 $(2j+\mu,\mu)$, 有

$$k_{(2i+\tau,\tau)}=k_{(2j+\mu,\mu)}\Longleftrightarrow n=4j+3, i=j+1,\tau=0\text{和}\,\mu=1.$$

现在假定 $n=4j+3$. 当 $n=3$ 时, 我们取 $i=1$, $j=0$, $\tau=0$ 和 $\mu=1$. 如果 $f:R_{(1,1)}(3)\to R_{(2,0)}(3)$, 那么由定理 1.27,

$$p^{(2,0)}_{(2,0)(2,0)}(3)=p^{(1,1)}_{(1,1)(1,1)}(3).$$

直接计算可知上式等号左边等于 $q-1$, 而右边等于 q^3-1. 所以这种情形不会出现.

当 $n\geqslant3$ 时, 如果 f 把关系 $R_{(2j+1,1)}(n)$ 变成 $R_{(2j+2,0)}(n)$, 而保持其余所有关系不变, 那么

$$p^{(2j+2,0)}_{(1,1)(2j+2,0)}(n)=p^{(2j+1,1)}_{(1,1)(2j+1,1)}(n).$$

注意到上式等号左边等于 0, 而右边不等于 0, 所以这种情形也不会出现. 因此 f 保持 Sym(n, q) 的每个关系不变. 于是

$$\text{InnSym}(n,q)=\text{AutSym}(n,q).\qquad\square$$

从定理 6.13 知, 当 q 为 2 的方幂时, Sym(n, q) 的聚合方案 $\overline{\text{Sym}}(n,q)$ 与 $\mathbb{F}_q$ 上 $n+1$ 阶交错矩阵的结合方案 Alt$(n+1, q)$ 同构. 而 Alt$(n+1, q)$ 的自同构已由定理 3.17 给出了, 自然, 我们可以利用定理 6.13 中的映射 ψ 给出 $\overline{\text{Sym}}(n,q)$ 的自同构形状.

第七章　二次型结合方案 (特征数＝2)

§7.1　二次型的标准形式和结合方案

我们知道, 奇特征数的域 $\mathbb{F}_q$ 上的 n 元二次型可以用 $\mathbb{F}_q$ 上的 $n\times n$ 对称矩阵来表示. 然而, 对于特征数为 2 的域 $\mathbb{F}_q$ 上的二次型来说, 情况却不是这样. 在这一章中, 我们恒设 $\mathbb{F}_q$ 是特征数为 2 的 q 元域, 即 q 是 2 的幂.

定义　设 V 是 $\mathbb{F}_q$ 上的一个 n 维向量空间.V 到 $\mathbb{F}_q$ 的函数 f 称为 V 上的一个*二次型*, 如果满足如下条件:

(1) $f(au)=a^2f(u)$, $\forall a\in\mathbb{F}_q$, $\forall u\in V$.

(2) $f(u+v)=f(u)+f(v)+B_f(u,v)$, $\forall u,v\in V$, 这里 B_f 是 V 上的一个*相伴于 f 的对称双线性型*.

在条件 (1) 中, 如果取 $a=0$, 立得 $f(0)=0$. 在条件 (2) 中取 $u=v$, 并注意到 $\mathbb{F}_q$ 的特征数为 2, 立得 $B_f(u,u)=0$, $\forall u\in V$. 因而 B_f 是交错的.

现在取定 V 的一个基 $e_1,e_2,\cdots,e_n$. 令 $a_i=f(e_i)$, $b_{ij}=B_f(e_i,e_j)$. 那么, 对于 V 的任意向量 $u=x_1e_1+\cdots+x_ne_n$, 由定义中的条件 (1) 和 (2) 可得

$$f(u)=\sum_{i=1}^{n}a_ix_i^2+\sum_{1\leqslant i<j\leqslant n}b_{ij}x_ix_j.$$

这样, 二次型 f 在取定的基下可表示成坐标 $x_1,\cdots,x_n$ 的一个二次齐式. 令 $a_{ii}=a_i$, $a_{ij}=b_{ij}(i<j)$ 及 $a_{ij}=0(i>j)$, 那么二次型 f 对应一个上三角矩阵 $A=(a_{ij})$, 并且

$$f(u)=\sum_{1\leqslant i\leqslant j\leqslant n}a_{ij}x_ix_j. \tag{7.1}$$

如果写成矩阵形式, 即有 $f(u)=(x_1,\cdots,x_n)A\,{}^t(x_1,\cdots,x_n)$, 那么相伴于 f 的交错型 B_f 在这个基之下的矩阵就是 $A+{}^tA$.

我们取 V 的另外一个基 $v_1,v_2,\cdots,v_n$. 设向量 $u=y_1v_1+\cdots+y_nv_n$, 并设坐标间的转换矩阵为 T, 即 $(x_1,\cdots,x_n)=(y_1,\cdots,y_n)T$. 那么二次型 f 在基 $v_1,\cdots,v_n$ 之下对应的 n 元二次齐式为 $f(u)=(y_1,\cdots,y_n)(TA\,{}^tT)\,{}^t(y_1,\cdots,y_n)$. 将此式中的同类项合并成形如 (7.1), 我们就得到与 f 对应的上三角矩阵 B. 现在, 我们来叙述二次型的矩阵说法.

设 $n\geqslant 1$ 是整数. 令 M_n 表示 $\mathbb{F}_q$ 上全体 $n\times n$ 矩阵所成的集合, K_n 表示 $\mathbb{F}_q$ 上全体 $n\times n$ 交错矩阵所成的集合. 称 M_n 中两个矩阵 A 和 B 模 K_n同余, 如果

$A-B\in K_n$, 记作 $A\equiv B \pmod{K_n}$, 或简单记作 $A\equiv B$. 这是 M_n 上的一个等价关系, A 所在的等价类记作 [A].

称 M_n 中两个矩阵 A 和 B 是"合同"的, 记作 $A\sim B$, 如果存在一个 $n\times n$ 的非奇异矩阵 T 使得 $TA{}^tT\equiv B$. 显然, 如果 A 与 B"合同", 那么与 A 同余的任一矩阵均与 B"合同". 我们也可记作 $[A]\sim[B]$.

这样, 在取定 V 的一个基之下, V 上的二次型与 M_n 模 K_n 的同余类一一对应, 而改变 V 的基, 相当于 $[A]$ 的合同变换. 以后谈到二次型指的就是矩阵的同余类. 在讨论中, 为了方便, 我们常将 n 元二次型所对应的矩阵类 $[A]$ 的代表元取为上三角形矩阵 A, 有时也用 A 来表示这个 n 元二次型.

下面我们讨论 $\mathbb{F}_q$ 上矩阵的"合同"标准形. 由于 $\mathbb{F}_q$ 中的元素皆为平方元, 任意 1 阶非零矩阵均"合同"于 (1). 对于 2 阶矩阵, 我们有

定理 7.1　设 2×2 矩阵 $A=\begin{pmatrix} a & b\\ & c\end{pmatrix}\neq 0$. 那么

$$A\sim\begin{cases}\begin{pmatrix}1 & \\ & 0\end{pmatrix}, & \text{如果 } b=0, (a,c \text{ 不全为 } 0),\\ \begin{pmatrix}0 & 1\\ & 0\end{pmatrix}, & \text{如果 } b\neq 0,\ b^{-2}ac\in N,\\ \begin{pmatrix}\alpha & 1\\ & \alpha\end{pmatrix}, & \text{如果 } b\neq 0, b^{-2}ac\notin N,\end{cases}$$

这里 α 是 $\mathbb{F}_q$ 中不属于 $N=\{x^2+x|x\in\mathbb{F}_q\}$ 的一个固定元.

证明　设 $b=0$, 于是 a,c 不全为 0. 不妨设 $a\neq 0$. 取 $x\in\mathbb{F}_q$ 使 $ax^2=c$, 那么有

$$\begin{pmatrix}a^{-\frac12} & 0\\ x & 1\end{pmatrix}\begin{pmatrix}a & \\ & c\end{pmatrix}\begin{pmatrix}a^{-\frac12} & x\\ 0 & 1\end{pmatrix}\equiv\begin{pmatrix}1 & \\ & 0\end{pmatrix}.$$

如果 $a=0$, 那么 $c\neq 0$. 这时考虑

$$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}0 & \\ & c\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\equiv\begin{pmatrix}c & \\ & 0\end{pmatrix}.$$

现在, 设 $b\neq 0$, 而 $b^{-2}ac\in N$. 如果 $c=0$, 那么

$$\begin{pmatrix}b^{-1} & ab^{-2}\\ 0 & 1\end{pmatrix}\begin{pmatrix}a & b\\ & 0\end{pmatrix}\begin{pmatrix}b^{-1} & 0\\ ab^{-2} & 1\end{pmatrix}\equiv\begin{pmatrix}0 & 1\\ & 0\end{pmatrix}.$$

设 $c\neq 0$, 由 $b^{-2}ac\in N$, 存在 $y\in\mathbb{F}_q$ 使得 $b^{-2}ac=y^2+y$, 这时, 我们有

$$\begin{pmatrix}b^{-1} & c^{-1}y\\ 0 & 1\end{pmatrix}\begin{pmatrix}a & b\\ & c\end{pmatrix}\begin{pmatrix}b^{-1} & 0\\ c^{-1}y & 1\end{pmatrix}\equiv\begin{pmatrix}0 & 1\\ & c\end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ & c \end{pmatrix} \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} 0 & 1 \\ & 0 \end{pmatrix}.$$

最后，设 $b \neq 0$ 而 $b^{-2}ac \notin N$. 这时自然有 $ac \neq 0$. 我们证明存在 2×2 可逆矩阵 $\begin{pmatrix} \lambda & 0 \\ x & \mu b^{-1} \end{pmatrix}$ 使得

$$\begin{pmatrix} \lambda & 0 \\ x & \mu b^{-1} \end{pmatrix} \begin{pmatrix} a & b \\ & c \end{pmatrix} \begin{pmatrix} \lambda & x \\ 0 & \mu b^{-1} \end{pmatrix} \equiv \begin{pmatrix} \alpha & 1 \\ & \alpha \end{pmatrix}$$

成立. 如果上式成立，那么应有

$$a\lambda^2 = \alpha,\ \lambda\mu = 1,\ ax^2 + \mu x + c\mu^2 b^{-2} = \alpha.$$

由第一个式子知，$\lambda = (a^{-1}\alpha)^{\frac{1}{2}}$. 由第二个式子，$\mu = \lambda^{-1} = (a\alpha^{-1})^{\frac{1}{2}}$. 这时，第三个式子为 $ax^2 + (a\alpha^{-1})^{\frac{1}{2}}x + b^{-2}ac\alpha^{-1} = \alpha$. 两边乘以 α, 有 $a\alpha x^2 + (a\alpha)^{\frac{1}{2}}x + b^{-2}ac = \alpha^2$. 由于 $\alpha \notin N$ 知 $\alpha^2 \notin N$, 而 $b^{-2}ac \notin N$ 且 $\mathbb{F}_q : N = 2$, 所以 $b^{-2}ac + \alpha^2 \in N$, 于是有 y 使 $b^{-2}ac + \alpha^2 = y^2 + y$. 取 $x = y(a\alpha)^{-\frac{1}{2}}$ 即可. □

对于任意一个 $n \times n$ 矩阵 $A = (a_{ij}) \neq 0$, 这里 $a_{ij} = 0 (i > j), n \geqslant 3$. 若对任意 $i < j$, $a_{ij} = 0$, 则容易得到 A "合同" 于矩阵 $[1,\ 0^{(n-1)}]$; 否则，存在 $a_{ij} \neq 0, i \neq j$. 通过互换矩阵 A 的 $1, i$ 两行和 $1, i$ 两列，再互换 $2, j$ 两行和 $2, j$ 两列，不妨设 $a_{12} \neq 0$. 将第二列的 $a_{12}^{-1}a_{1k}$ 倍加到 A 的第 $k (k = 3, \cdots, n)$ 列, 再对 A 作相应的行变换之后，我们可以假设 $a_{1k} = 0, k = 3, \cdots, n$. 再将第一行的 $a_{12}^{-1}a_{2k}$ 倍加到 A 的第 $k (k = 3, \cdots, n)$ 行, 再对 A 作相应的列变换之后，不妨设矩阵 A "合同" 于矩阵 $\left[\begin{pmatrix} a_{11} & a_{12} \\ & a_{22} \end{pmatrix}, B\right]$, 这里 B 是一个 $(n-2) \times (n-2)$ 上三角矩阵. 注意到

$$\left[\begin{pmatrix} \alpha & 1 \\ & \alpha \end{pmatrix}, 1\right] \sim \left[\begin{pmatrix} 0 & 1 \\ & 0 \end{pmatrix}, 1\right],$$

$$\left[\begin{pmatrix} \alpha & 1 \\ & \alpha \end{pmatrix}, \begin{pmatrix} \alpha & 1 \\ & \alpha \end{pmatrix}\right] \sim \left[\begin{pmatrix} 0 & 1 \\ & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ & 0 \end{pmatrix}\right].$$

对 n 应用归纳法, 不难得到如下定理的部分内容.

定理 7.2(L.E.Dickson) $\mathbb{F}_q$ 上任一 $n \times n$ 矩阵都恰 "合同" 于如下形式矩阵之一

$$\left[\begin{pmatrix} 0 & I^{(\nu)} \\ & 0 \end{pmatrix}, 0^{(n-2\nu)}\right], \left[\begin{pmatrix} 0 & I^{(\nu)} \\ & 0 \end{pmatrix}, 1, 0^{(n-2\nu-1)}\right],$$

$$\left[\begin{pmatrix} 0 & I^{(\nu)} \\ & 0 \end{pmatrix}, \begin{pmatrix} \alpha & 1 \\ & \alpha \end{pmatrix}, 0^{(n-2\nu-2)}\right],$$

这里 α 是 $\mathbb{F}_q$ 中不属于 $N = \{x^2 + x | x \in \mathbb{F}_q\}$ 的一个固定元.ν 称为指数.

对于此定理. 余下的只需证明定理中所述三种类型的矩阵彼此不 "合同" 即可. 对此可参考文献 [15] 的定理 1.34, 这里不再赘述.

上述三种矩阵统一说成是$(2\nu+\delta,\nu)$ 型的, 这里 $\delta=0,1$ 或 2. 它们的"秩"定义为 $2\nu+\delta$. 如果"秩"等于 n, 那么该矩阵称为*正则的*. 我们把类型 $(2\nu,\nu)$, $(2\nu+1,\nu)$ 和 $(2\nu+2,\nu)$ 分别简记为 $2\nu^+, 2\nu+1$ 和 $2\nu+2^-$(或 $2(\nu+1)^-$). 这样, n 元二次型的类型为 $0, 1, 2^+, 2^-, 3, 4^+, \cdots$. 非零的类型共有 $n+[n/2]$ 个. 为了讨论方便, 我们把 n 元二次型 A 的类型及其所对应矩阵类中矩阵的类型记为 $t(A)$. 例如, 当 A 的类型为 2^- 时, 就记为 $t(A)=2^-$.

$\mathbb{F}_q$ 上的 $n\times n$ 矩阵 A 称为*定号的*, 如果从 $xA\,{}^tx=0$, $x\in\mathbb{F}_q^{(n)}$ 推出 $x=0$, 否则称为非定号的. 从定理 7.1 可知, $\mathbb{F}_q$ 上的定号矩阵的级数 $\leqslant 2$. 如果定号矩阵 A 是 1×1 矩阵, A 一定"合同"于 (1). 如果 A 是 2×2 定号矩阵, A 一定"合同"于 $\begin{pmatrix}\alpha & 1\\ & \alpha\end{pmatrix}$. 实际上, 假如 $x=(x_1,\,x_2)\neq 0$ 而有 $(x_1\quad x_2)\begin{pmatrix}\alpha & 1\\ & \alpha\end{pmatrix}\begin{pmatrix}x_1\\ x_2\end{pmatrix}=\alpha x_1^2+x_1x_2+\alpha x_2^2=0.$ 不妨设 $x_1\neq 0$, 那么推出 $\alpha^2=(\alpha x_1^{-1}x_2)^2+(\alpha x_1^{-1}x_2)\in N$, 因而 $\alpha\in N$, 导致矛盾.

我们用 $Q(n,\,q)$ 表示 $\mathbb{F}_q$ 上全体 n 元二次型的集合. $Q(n,\,q)$ 可以看作 $M_n(\mathbb{F}_q)$ 模子空间 K_n 所得商空间, 因而 $Q(n,\,q)$ 自然带有向量空间结构, 且

$$\dim_{\mathbb{F}_q} Q(n,q)=\frac{1}{2}n(n+1).$$

令 $G=GL_n(\mathbb{F}_q)\ltimes Q(n,q)$, 即 $GL_n(\mathbb{F}_q)$ 关于加法群 $Q(n,q)$ 的半直积, G 中的乘法为

$$(T,\,[A])(P,\,[B])=(TP,[TB\,{}^tT+A]).$$

现在, G 如下自然地作用在 $Q(n,\,q)$ 上,

$$\begin{aligned} G\times Q(n,\,q) &\longrightarrow Q(n,q)\\ ((T,\,[A]),\,X) &\longmapsto [TX\,{}^tT]+[A]. \end{aligned}\tag{7.2}$$

G 就是由作用在 $Q(n,\,q)$ 上的线性群 $GL_n(\mathbb{F}_q)$ 和 $Q(n,\,q)$ 的平移群生成的群. 显然, G 作用在 $Q(n,\,q)$ 上是可迁的. 于是 $(G,\,Q(n,\,q))$ 决定 $Q(n,\,q)$ 上的一个结合方案, 记作 $\mathrm{Qua}(n,\,q)$, 我们把它叫做 $\mathbb{F}_q$ 上的*二次型结合方案*. 两个二次型对子 $([A_1],\,[A_2])$ 和 $([B_1],\,[B_2])$ 在 $\mathrm{Qua}(n,\,q)$ 的同一个结合类当且仅当存在 $T\in GL_n(\mathbb{F}_q)$, 使得 $T(A_1-A_2)\,{}^tT\equiv B_1-B_2 \pmod{K_n}$. 由此可知, $\mathrm{Qua}(n,\,q)$ 的结合类恰由 $Q(n,\,q)$ 的"合同类"所决定, 即二次型的类型来决定. 如果 A_1-A_2 的类型为 i, $i\in J=\{0,\,1,\,2^+,\,2^-,\,3,\,\cdots\}$, 我们就把 $([A_1],\,[A_2])$ 所在的结合类记为 R_i. 由于 $A_1-A_2=A_2-A_1$, 所以 R_i 都是对称的.$\mathrm{Qua}(n,\,q)$ 的非平凡结合类的个数是 $n+[\frac{n}{2}]$. 如果 n 为奇数, 那么 $J=\{0,\,1,\,2^+,\,2^-,\,\cdots,n\}$; 如果 n 为偶数, 那么 $J=\{0,\,1,\,2^+,\,2^-,\,\cdots,\,n^+,\,n^-\}$. 我们将 $Qua(n,q)$ 的价 k_i 记作 $k_i(n)$, 将交叉数 p_{ij}^k 记作 $p_{ij}^k(n)$. 但在上下文意义明显时, n 也可省略不写.

§7.2　Qua (2, q) 和 Qua (3, q) 的参数

在下面的几节中，我们要讨论 Qua(n, q) 的参数. 本节讨论 $n = 2,3$ 的情形. 由于涉及到 $N = \{x^2 + x | x \in \mathbb{F}_q\}$ 的某些计数, 所以我们先对 N 的性质作一些讨论.

注意到 N 对加法是封闭的, 因而是 $\mathbb{F}_q$ 的加法群的一个子群. 又映射 $x \mapsto x^2+x$ 是从 $\mathbb{F}_q$ 到 N 的一个加法群同态，它的核为 $\{0,1\}$, 因此 $\mathbb{F}_q : N = 2$, 于是 $|N| = \frac{1}{2}q$. 进一步由 $F_q^2 = \mathbb{F}_q$ 可知 $N^2 = N$.

设 $q = 2^t$, t 为正整数. $\mathbb{F}_q$ 在 $\mathbb{F}_2$ 上的 Galois 群为 t 阶循环群 $\langle\eta\rangle$, 这里 η 为 Frobenius 映射 $\eta(x) = x^2, \forall x \in \mathbb{F}_q$. $\mathbb{F}_q$ 在 $\mathbb{F}_2$ 的迹(*trace*), 记为 Tr, 为从 $\mathbb{F}_q$ 到 $\mathbb{F}_2$ 的如下映射

$$\mathrm{Tr}(x) = x + x^{\eta} + \cdots + x^{\eta^{t-1}}, \forall x \in \mathbb{F}_q. \tag{7.3}$$

Tr 为线性的. 易见, $N \subseteq \mathrm{Ker(Tr)}$. 利用 Hilbert Satz 90 的加法形式可知 $N = \mathrm{Ker(Tr)}$ (参看 N. Jacobson. Basic Algebraic I. Theorem 4.31). 利用 Tr 定义 $\mathbb{F}_q$ 上的一个对称内积：

$$(x, y) = \mathrm{Tr}(xy), \forall x, y \in \mathbb{F}_q. \tag{7.4}$$

这个内积是非退化的, 因为如果 $(a, y) = 0$, $\forall y \in \mathbb{F}_q$, 那么就有 $a\mathbb{F}_q \subseteq N$, 而 $|N| = \frac{1}{2}q$, 必有 $a = 0$.

由于 N 是 $\mathbb{F}_q$ 的一个子空间且 $|N| = \frac{1}{2}q = 2^{t-1}$, 所以 N 是 $\mathbb{F}_q$ 的一个超平面. 对于任意 $a \in \mathbb{F}_q^*$, aN 也是 $\mathbb{F}_q$ 的加法子群且 $|aN| = \frac{1}{2}q$, 所以 aN 是 $\mathbb{F}_q$ 的一个超平面. 注意到 aN 关于内积 $(,)$ 的正交补 $(aN)^{\perp} = \langle a^{-1}\rangle$, 其中非 0 元素仅有一个, 即 a^{-1}. $\mathbb{F}_q$ 的每个超平面均可如此得到. 对于 $a \in \mathbb{F}_q^*$ 及 $b \in \mathbb{F}_q$, $aN + b$ 是 $\mathbb{F}_q$ 的仿射超平面.

定理 7.3　设 $\mathbb{F}_q$ 是 q 元有限域, $q = 2^t \geqslant 2$, $N = \{x^2+x | x \in \mathbb{F}_q\}$. 设 $a_1, \cdots, a_r$ 均不为 0, 而 $b_1, \cdots, b_r$ 任意. 那么

$$|(a_1N + b_1) \cap (a_2N + b_2) \cap \cdots \cap (a_rN + b_r)| = 2^{t-r}$$

当且仅当 $a_1^{-1}, \cdots, a_r^{-1}$ 在 $\mathbb{F}_2$ 上线性无关.

证明　记 $P = \cap_{i=1}^{r}(a_iN + b_i)$. 那么 P 是非齐次线性方程组

$$\begin{cases} (a_1^{-1}, x) = (a_1^{-1}, b_1), \\ (a_2^{-1}, x) = (a_2^{-1}, b_2), \\ \cdots\cdots\cdots\cdots \\ (a_r^{-1}, x) = (a_r^{-1}, b_r) \end{cases}$$

的解集. 由线性方程组相容性判别定理立得本定理. □

(I) 二元二次型结合方案的参数.

定理 7.4 关于二元二次型结合方案的参数, 我们有

$$k_0=1,\ \ k_1=q^2-1,\ \ k_{2^+}=\frac{1}{2}q(q^2-1),\ \ k_{2^-}=\frac{1}{2}q(q-1)^2.$$

$$B_1=\begin{pmatrix} 0 & 1 & 0 & 0 \\ q^2-1 & q^2-2 & 0 & 0 \\ 0 & 0 & \frac{1}{2}(q-1)(q+2) & \frac{1}{2}q(q+1) \\ 0 & 0 & \frac{1}{2}q(q-1) & \frac{1}{2}(q+1)(q-2) \end{pmatrix},$$

$$B_{2^+}=\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & \frac{1}{2}(q-1)(q+2) & \frac{1}{2}q(q+1) \\ \frac{1}{2}q(q^2-1) & \frac{1}{4}q(q-1)(q+2) & \frac{1}{4}q(q-2)(q+3) & \frac{1}{4}q(q+1)(q-2) \\ 0 & \frac{1}{4}q^2(q-1) & \frac{1}{4}q(q-1)(q-2) & \frac{1}{4}q(q+1)(q-2) \end{pmatrix},$$

$$B_{2^-}=\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & \frac{1}{2}q(q-1) & \frac{1}{2}(q+1)(q-2) \\ 0 & \frac{1}{4}q^2(q-1) & \frac{1}{4}q(q-1)(q-2) & \frac{1}{4}q(q+1)(q-2) \\ \frac{1}{2}q(q-1)^2 & \frac{1}{4}q(q-1)(q-2) & \frac{1}{4}q(q-1)(q-2) & \frac{1}{4}q(q-2)(q-3) \end{pmatrix}.$$

证明 从定理 7.1 可以算出 k_i 之值. 关于交叉数, 我们仅以计算 $p_{12^+}^{2^+}$, $p_{2^+2^+}^{2^+}$ 和 $p_{2^+2^-}^{2^-}$ 为例, 其余的可以类似地得出.

(1) $p_{12^+}^{2^+}$ 的计算.

令 $A_1=0, A_2=\begin{pmatrix} 0 & 1 \\ & 0 \end{pmatrix}, A=\begin{pmatrix} a & 0 \\ & d \end{pmatrix}$, 这里 a,d 不全为 0. 那么

$$p_{12^+}^{2^+}=|\{A|t(A+A_2)=2^+\}|,$$

于是

$$p_{12^+}^{2^+}=|\{(a,d)|ad\in N\ \text{这里}\ a,d\ \text{不全为}\ 0\}|.$$

因此, 当 $a=0$ 时, d 有 $q-1$ 种取法; 当 $a\neq 0$ 时, a 有 $q-1$ 种取法, 对于取定的 a, 因为 $d\in a^{-1}N$, d 有 $|a^{-1}N|=\frac{1}{2}q$ 种取法. 这样就可算出

$$p_{12^+}^{2^+} = \frac{1}{2}(q-1)(q+2).$$

(2) $p_{2^+2^+}^{2^+}$ 的计算.

令 $A_1 = 0$, $A_2 = \begin{pmatrix} 0 & 1 \\ & 0 \end{pmatrix}$, $A = \begin{pmatrix} a & b \\ & c \end{pmatrix}$, 那么

$$p_{2^+2^+}^{2^+} = |\{A | t(A + A_2) = 2^+, t(A) = 2^+\}|.$$

由此可知

$$p_{2^+2^+}^{2^+} = |\{(a,b,c) | b \neq 0, 1;\ b^{-2}ac \in N; (b+1)^{-2}ac \in N\}|.$$

由 $b \neq 0, 1$, 可知 b 有 $q-2$ 种取法. 一但 b 取定之后, 当 $a = 0$ 时, c 有 q 种取法; 当 $a \neq 0$ 时, 根据定理 7.3, c 有 $\frac{1}{4}q$ 种取法. 于是

$$p_{2^+2^+}^{2^+} = \frac{1}{4}q(q-2)(q+3).$$

(3) $p_{2^+2^-}^{2^-}$ 的计算.

令 $A_1 = 0, A_2 = \begin{pmatrix} \alpha & 1 \\ & \alpha \end{pmatrix}$, $A = \begin{pmatrix} a & b \\ & c \end{pmatrix}$, 那么

$$p_{2^+2^-}^{2^-} = |\{A | t(A + A_2) = 2^-, t(A) = 2^+\}|.$$

由此可知

$$p_{2^+2^-}^{2^-} = |\{(a,b,c) | b \neq 0, 1;\ b^{-2}ac \in N; (b+1)^{-2}(a+\alpha)(c+\alpha) \notin N\}|.$$

因为 $b \neq 0, 1$, 所以 b 有 $q-2$ 种取法. 一但 b 取定之后, 当 $a = 0$ 时, c 有 $\frac{1}{2}q$ 种取法; 若 $a = \alpha$, 则条件 $(b+1)^{-2}(a+\alpha)(c+\alpha) \notin N$ 不成立, 因而 $a \neq \alpha$.

现在 $a \neq 0, \alpha$. 考虑 $|b^2a^{-1}N \cap (\alpha + (b+1)^2(a+\alpha)^{-1}N)|$. 注意到

$$b^2a^{-1} = (b+1)^2(a+\alpha)^{-1} \Longleftrightarrow b^2(a+\alpha) = (b+1)^2 a \Longleftrightarrow b^2\alpha = a.$$

进一步, 当 $b^2\alpha = a$ 时,

$$b^2a^{-1}N \cap (\alpha + (b+1)^2(a+\alpha)^{-1}N) = \varnothing.$$

因此, c 只要求满足 $b^{-2}ac \in N$, 故 c 有 $\frac{1}{2}q$ 种取法.

对于 $a \neq 0$, α 和 $b^2\alpha$, 这时 $b^2a^{-1} \neq (b+1)^2(a+\alpha)^{-1}$, 由定理 7.3,

$$|b^2a^{-1}N \cap (\alpha + (b+1)^2(a+\alpha)^{-1}N)| = \frac{1}{4}q,$$

所以, 对于 a 来说, c 有 $\frac{1}{4}q$ 种取法.

综上讨论, 就得到

$$p_{2^+2^-}^{2^-} = (q-2)\left[\frac{q}{2} + \frac{q}{2} + (q-3)\frac{q}{4}\right] = \frac{1}{4}q(q+1)(q-2). \qquad \square$$

(II) 三元二次型结合方案的参数.

定理 7.5 设 $A=\begin{pmatrix} a & b & v_1 \\ & c & v_2 \\ & & u \end{pmatrix} \neq 0$, 那么

(1) 当 $v_1=v_2=0$ 时,

$$t(A)=\begin{cases} 1, & \text{如果 } b=0, a, c, u \text{ 不全为} 0, \\ 2^+(2^-), & \text{如果 } b\neq 0,\ u=0,\ b^{-2}ac\in N(\notin N), \\ 3, & \text{如果 } b\neq 0,\ u\neq 0. \end{cases}$$

(2) 当 $v_1=0, v_2\neq 0$ 时,

$$t(A)=\begin{cases} 2^+(2^-), & \text{如果 } a=v_2^{-2}b^2u,\ v_2^{-2}cu\in N(v_2^{-2}cu\notin N), \\ 3, & \text{如果 } a\neq v_2^{-2}b^2u. \end{cases}$$

(3) 当 $v_1\neq 0$ 时,

$$t(A)=\begin{cases} 2^+(2^-), & \text{如果 } c=v_1^{-2}v_2^2a+v_1^{-1}v_2b+v_1^{-2}b^2u, \\ & \qquad v_1^{-2}au\in N(v_1^{-2}au\notin N), \\ 3, & \text{如果 } c\neq v_1^{-2}v_2^2a+v_1^{-1}v_2b+v_1^{-2}b^2u. \end{cases}$$

证明 (1) 的结果是显然的.

(2) 由于

$$\begin{pmatrix} 1 & & v_2^{-1}b \\ & 1 & \\ & & 1 \end{pmatrix}\begin{pmatrix} a & b & 0 \\ & c & v_2 \\ & & u \end{pmatrix}\begin{pmatrix} 1 & & \\ & 1 & \\ v_2^{-1}b & & 1 \end{pmatrix} \equiv \begin{pmatrix} a+v_2^{-2}b^2u & 0 & 0 \\ & c & v_2 \\ & & u \end{pmatrix},$$

所以 (2) 的结论成立.

(3) 由于

$$\begin{pmatrix} 1 & & \\ v_1^{-1}v_2 & 1 & v_1^{-1}b \\ & & 1 \end{pmatrix}\begin{pmatrix} a & b & v_1 \\ & c & v_2 \\ & & u \end{pmatrix}\begin{pmatrix} 1 & v_1^{-1}v_2 & \\ & 1 & \\ & v_1^{-1}b & 1 \end{pmatrix} \equiv \begin{pmatrix} a & 0 & v_1 \\ & c^* & 0 \\ & & u \end{pmatrix},$$

这里 $c^*=c+v_1^{-2}v_2^2a+v_1^{-1}v_2b+v_1^{-2}b^2u$, 所以 (3) 的结论成立. □

定理 7.6 关于三元二次型结合方案的参数, 我们有

$$k_0 = 1,\ k_1 = q^3 - 1,\ k_{2+} = \frac{1}{2}q(q+1)(q^3-1),$$

$$k_{2-} = \frac{1}{2}q(q-1)(q^3-1),\ k_3 = q^2(q-1)(q^3-1).$$

$$B_1 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ e & q^3-2 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{2}ad & \frac{1}{2}qb & \frac{1}{2}qb \\ 0 & 0 & \frac{1}{2}qa & \frac{1}{2}bc & \frac{1}{2}qa \\ 0 & 0 & q^2a & q^2a & f \end{pmatrix},$$

$$B_{2+} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{2}ad & \frac{1}{2}qb & \frac{1}{2}qb \\ \frac{1}{2}qbe & \frac{1}{4}qabd & \frac{1}{4}q(q+3)g & \frac{1}{4}qbc & \frac{1}{4}qabd \\ 0 & \frac{1}{4}q^2ab & \frac{1}{4}qac & \frac{1}{4}qbg & \frac{1}{4}q^2ab \\ 0 & \frac{1}{2}q^3ab & \frac{1}{2}q^2a^2d & \frac{1}{2}q^3ab & \frac{1}{2}qbf \end{pmatrix},$$

$$B_{2-} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & \frac{1}{2}qa & \frac{1}{2}bc & \frac{1}{2}qa \\ 0 & \frac{1}{4}q^2ab & \frac{1}{4}qac & \frac{1}{4}qbg & \frac{1}{4}q^2ab \\ \frac{1}{2}qae & \frac{1}{4}qabc & \frac{1}{4}qag & \frac{1}{4}qc(q-3) & \frac{1}{4}qabc \\ 0 & \frac{1}{2}q^3a^2 & \frac{1}{2}q^3a^2 & \frac{1}{2}q^2abc & \frac{1}{2}qaf \end{pmatrix},$$

$$B_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & q^2a & q^2a & f \\ 0 & \frac{1}{2}q^3ab & \frac{1}{2}q^2a^2d & \frac{1}{2}q^3ab & \frac{1}{2}qbf \\ 0 & \frac{1}{2}q^3a^2 & \frac{1}{2}q^3a^2 & \frac{1}{2}q^2abc & \frac{1}{2}qaf \\ q^2ae & q^2af & q^2af & q^2af & q^2(af-c) \end{pmatrix},$$

这里, $a = q-1$, $b = q+1$, $c = q-2$, $d = q+2$, $e = q^3-1$, $f = q^3-q^2-1$, $g = 2q^2-q-2$.

证明 利用定理 7.5 容易算出价 k_i 之值. 关于交叉数, 我们仅以计算 $p_{2^+2^+}^{2^+}(3)$, $p_{2^-3}^{2^-}(3)$, $p_{33}^{3}(3)$ 为例, 其余的可类似地得出.

(1) $p_{2^+2^+}^{2^+}(3)$ 的计算.

令 $A_1 = 0$, $A_2 = \begin{pmatrix} 0 & 1 & \\ & 0 & \\ & & 0 \end{pmatrix}$, $A = \begin{pmatrix} a & b & v_1 \\ & c & v_2 \\ & & u \end{pmatrix}$, 那么

$$p_{2^+2^+}^{2^+}(3) = |\{A \in Q(3,q) | t(A+A_2) = 2^+, t(A) = 2^+\}|.$$

应用定理 7.5, 有如下结论

1) 如果 $v_1 = v_2 = 0$, 那么 $u = 0$, 于是满足要求的矩阵 A 的个数为 $p_{2^+2^+}^{2^+}(2)$. 由定理 7.4, 有

$$p_{2^+2^+}^{2^+}(2) = \frac{1}{4}q(q-2)(q+3).$$

2) 如果 $v_1 = 0$, $v_2 \neq 0$, 那么满足要求的矩阵 A 的个数为

$$|\{(a,b,c,v_2,u) | v_2^{-2}cu \in N, a + v_2^{-2}b^2u = 0, a + v_2^{-2}(b^2+1)u = 0\}| = q^2(q-1).$$

3) 如果 $v_1 \neq 0$, 那么满足要求的矩阵 A 的个数为

$$|\{(a,b,c,v_1,v_2,u) | v_1^{-2}au \in N,\ t = 0, v_1^{-2}u + v_1^{-1}v_2 = 0\}|,$$

这里 $t = c + v_1^{-2}v_2^2a + v_1^{-1}v_2b + v_1^{-2}b^2u$. 由 $v_1 \neq 0$, 知 v_1 有 $q-1$ 种取法. 在取定 v_1 之后, $a = 0$ 时, u 有 q 种取法; $a \neq 0$, 则 u 有 $\frac{1}{2}q$ 种取法. 一旦 v_1, a, u 都取定之后, v_2 随之确定, 而 b 有 q 种取法, c 则由条件所确定. 因此,

$$|\{(a,b,c,v_1,v_2,u) | v_1^{-2}au \in N, t = 0,\ v_1^{-2}u + v_1^{-1}v_2 = 0\}| = \frac{1}{2}q^2(q^2-1).$$

综上可得

$$p_{2^+2^+}^{2^+}(3)=\frac{1}{4}q(q+3)(2q^2-q-2).$$

(2) $p_{2^-3}^{2^-}(3)$ 的计算.

令 $A_1=0$, $A_2=\begin{pmatrix}\alpha & 1 & \\ & \alpha & \\ & & 0\end{pmatrix}$, $A=\begin{pmatrix}a & b & v_1\\ & c & v_2\\ & & u\end{pmatrix}$, 那么

$$p_{2^-3}^{2^-}(3)=|\{A\in Q(3,\,q)|t(A+A_2)=3,\,t(A)=2^-\}|.$$

应用定理 7.5, 我们可得

1) 如果 $v_1=v_2=0$, 那么满足要求的矩阵 A 的个数为 0.

2) 如果 $v_1=0$, $v_2\neq 0$, 那么满足要求的矩阵 A 的个数为

$$|\{(a,b,c,v_2,u)|v_2^{-2}cu\notin N,a+v_2^{-2}b^2u=0,v_2^{-2}u+\alpha\neq 0\}|=\frac{1}{2}q^2(q-1)(q-2).$$

3) 如果 $v_1\neq 0$, 那么满足要求的矩阵 A 的个数为

$$|\{(a,b,c,v_1,v_2,u)|v_1^{-2}au\notin N,t=0,v_1^{-2}u+v_1^{-1}v_2+\alpha+v_1^{-2}v_2^2\alpha\neq 0\}|$$

$$=\frac{1}{2}q^2(q-1)^2(q-2),$$

这里 $t=c+v_1^{-2}v_2^2a+v_1^{-1}v_2b+v_1^{-2}b^2u$.

综上可得

$$p_{2^-3}^{2^-}(3)=\frac{1}{2}q^2(q^2-1)(q-2).$$

(3) $p_{33}^{3}(3)$ 的计算.

令 $A_1=0$, $A_2=\begin{pmatrix}0 & 1 & \\ & 0 & \\ & & 1\end{pmatrix}$, $A=\begin{pmatrix}a & b & v_1\\ & c & v_2\\ & & u\end{pmatrix}$, 那么

$$p_{33}^{3}(3)=|\{A\in Q(3,q)|t(A+A_2)=3,t(A)=3\}|.$$

应用定理 7.5, 我们可得

1) 如果 $v_1=v_2=0$, 那么满足要求的矩阵 A 的个数为

$$|\{(a,b,c,u)|b\neq 0,1;\ u\neq 0,1;\ a,c\in\mathbb{F}_q\}|=q^2(q-2)^2.$$

2) 如果 $v_1=0$, $v_2\neq 0$, 那么满足要求的矩阵 A 的个数为

$$|\{(a,b,c,v_2,u)|a+v_2^{-2}v^2u\neq 0,a+v_2^{-2}b^2u+v_2^{-2}u+v_2^{-2}(b+1)^2\neq 0\}|$$

$$=(q-1)(q^4-2q^3+q^2).$$

3) 如果 $v_1 \neq 0$, 那么满足要求的矩阵 A 的个数为

$$
\begin{aligned}
&|\{(a,b,c,v_1,v_2,u)|t \neq 0, t+v_1^{-2}u+v_1^{-1}v_2+v_1^{-2}(b+1)^2 \neq 0\}| \\
&=(q-1)(q^5-2q^4+q^3),
\end{aligned}
$$

这里 $t=c+v_1^{-2}v_2^2a+v_1^{-1}v_2b+v_1^{-2}b^2u$.

综上可得

$$
p_{33}^3(3)=q^2(q^4-2q^3+q^2-2q+3). \qquad \square
$$

§7.3 特征数为 2 的正交空间的几个计数公式

设 G 是 $\mathbb{F}_q$ 上的一个 $n\times n$ 正则矩阵. $\mathbb{F}_q$ 上的矩阵 T 被称为关于 G 是正交的, 如果 $TG\,{}^tT\equiv G$. 显然, 关于 G 的 $n\times n$ 正交矩阵是非奇异的, 而且它们关于矩阵乘法作成一个群, 称为 $\mathbb{F}_q$ 上关于 G 的 *n 级正交群*, 记作 $O_n(\mathbb{F}_q,G)$. 易知, 如果 G_1 和 G_2 是 $\mathbb{F}_q$ 上两个“合同”的 $n\times n$ 正则矩阵, 那么 $O_n(\mathbb{F}_q,G_1)$ 和 $O_n(\mathbb{F}_q,G_2)$ 是同构的. $\mathbb{F}_q$ 上的 $n\times n$ 正则矩阵都“合同”于如下形式矩阵中的一个

$$
\begin{pmatrix} 0 & I^{(\nu)} \\ & 0 \end{pmatrix}, \quad \left[\begin{pmatrix} 0 & I^{(\nu)} \\ & 0 \end{pmatrix}, 1\right], \quad \left[\begin{pmatrix} 0 & I^{(\nu)} \\ & 0 \end{pmatrix}, \begin{pmatrix} \alpha & 1 \\ & \alpha \end{pmatrix}\right],
$$

这里 α 是 $\mathbb{F}_q$ 中取定的一个不属于 N 的固定元, 而且上面三个形式的正则矩阵彼此不“合同”. 这三种形式的矩阵统一记为

$$
G_{2\nu+\delta}=\left[\begin{pmatrix} 0 & I^{(\nu)} \\ & 0 \end{pmatrix}, \Delta\right], \tag{7.5}
$$

其中

$$
\Delta=\begin{cases} \varnothing(\text{可以略去不写}), & \text{如果 } \delta=0, \\ (1), & \text{如果 } \delta=1, \\ \begin{pmatrix} \alpha & 1 \\ & \alpha \end{pmatrix}, & \text{如果 } \delta=2. \end{cases}
$$

相应的正交群记为 $O_{2\nu+\delta}(\mathbb{F}_q)$, $\delta=0,1$ 或 2.(注: 文献中把 $\delta=0$ 和 $\delta=2$ 的正交群分别记为 $O_{2\nu}^+(q)$ 和 $O_{2(\nu+1)}^-(q)$.)

当 $\delta=1$ 时, $O_{2\nu+1}(\mathbb{F}_q)$ 中的元素具有形状

$$
\begin{pmatrix} A & B & P \\ C & D & Q \\ & & 1 \end{pmatrix}, \tag{7.6}
$$

这里 A, B, C, D 均为 ν 阶方阵，且

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in Sp_{2\nu}(\mathbb{F}_q),$$

P 和 Q 满足 $A\,{}^tB + P\,{}^tP \equiv 0, C\,{}^tD + Q\,{}^tQ \equiv 0$, 因而分别由 $A\,{}^tB$ 和 $C\,{}^tD$ 唯一确定，并且 $O_{2\nu+1}(\mathbb{F}_q)$ 与 $Sp_{2\nu}(\mathbb{F}_q)$ 同构 (参看 [15] 定理 7.1). 当 $\delta = 0$ 或 2 时，我们有

定理 7.7　对正交群 $O_{2\nu+\delta}(\mathbb{F}_q)(\delta = 0$ 或 $2)$ 来说，

$$T \in O_{2\nu+\delta}(\mathbb{F}_q) \Longleftrightarrow {}^tT \in O_{2\nu+\delta}(\mathbb{F}_q).$$

证明　分两种情形来证明：

i) $\delta = 0$.

如果 $T = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in O_{2\nu}(\mathbb{F}_q)$, 那么

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} 0 & I \\ 0 & 0 \end{pmatrix}\begin{pmatrix} {}^tA & {}^tC \\ {}^tB & {}^tD \end{pmatrix} \equiv \begin{pmatrix} 0 & I \\ 0 & 0 \end{pmatrix}.$$

由此可得

$$A\,{}^tB \equiv 0;\quad C\,{}^tD \equiv 0,\quad A\,{}^tD + B\,{}^tC = I.$$

注意到

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} {}^tD & {}^tB \\ {}^tC & {}^tA \end{pmatrix} = \begin{pmatrix} A\,{}^tD + B\,{}^tC & A\,{}^tB + B\,{}^tA \\ C\,{}^tD + D\,{}^tC & C\,{}^tB + D\,{}^tA \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix}.$$

即 $T^{-1} = \begin{pmatrix} {}^tD & {}^tB \\ {}^tC & {}^tA \end{pmatrix} \in O_{2\nu}(\mathbb{F}_q)$, 所以

$$\begin{pmatrix} {}^tD & {}^tB \\ {}^tC & {}^tA \end{pmatrix}\begin{pmatrix} 0 & I \\ 0 & 0 \end{pmatrix}\begin{pmatrix} D & C \\ B & A \end{pmatrix} \equiv \begin{pmatrix} 0 & I \\ 0 & 0 \end{pmatrix}.$$

于是

$${}^tDB \equiv 0;\quad {}^tCA \equiv 0;\quad {}^tDA +{}^t BC = I.$$

从而有

$$\begin{pmatrix} {}^tA & {}^tC \\ {}^tB & {}^tD \end{pmatrix}\begin{pmatrix} 0 & I \\ 0 & 0 \end{pmatrix}\begin{pmatrix} A & B \\ C & D \end{pmatrix} \equiv \begin{pmatrix} 0 & 0 \\ I & 0 \end{pmatrix}$$

于是有 ${}^tT \in O_{2\nu}(\mathbb{F}_q)$. 情形 i) 得证.

ii) $\delta = 2$.

先设 $\nu=0$, 即 $n=2$, $G=\begin{pmatrix}\alpha & 1\\ 0 & \alpha\end{pmatrix}$, α 是 $\mathbb{F}_q$ 中取定的一个不属于 N 的元素. 设 $T=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$. 那么 $T\in O_2^-(\mathbb{F}_q)(=O_2(\mathbb{F}_q,G))$ 当且仅当

$$\begin{cases}(a^2+b^2)\alpha+ab=\alpha,\\(c^2+d^2)\alpha+cd=\alpha,\\ad-bc=1.\end{cases}$$

当 $T\in O_2^-(\mathbb{F}_q)$ 时, 由于

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}d & b\\ c & a\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},$$

所以 $T^{-1}=\begin{pmatrix}d & b\\ c & a\end{pmatrix}\in O_2^-(\mathbb{F}_q)$. 因而

$$\begin{pmatrix}d & b\\ c & a\end{pmatrix}\begin{pmatrix}\alpha & 1\\ 0 & \alpha\end{pmatrix}\begin{pmatrix}d & c\\ b & a\end{pmatrix}\equiv\begin{pmatrix}\alpha & 1\\ 0 & \alpha\end{pmatrix}.$$

于是

$$\begin{cases}(b^2+d^2)\alpha+bd=\alpha,\\(a^2+c^2)\alpha+ac=\alpha,\\ad-bc=1.\end{cases}$$

这就推出

$$\begin{pmatrix}a & c\\ b & d\end{pmatrix}\begin{pmatrix}\alpha & 1\\ 0 & \alpha\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}\equiv\begin{pmatrix}\alpha & 1\\ 0 & \alpha\end{pmatrix}.$$

因此,

$$T\in O_2^-(\mathbb{F}_q)\Longleftrightarrow {}^tT\in O_2^-(\mathbb{F}_q).$$

再设 $\nu\geqslant 1$. 由 [5] 第十章第四节定理 2, 正交群 $O_{2\nu+2}(\mathbb{F}_q)$ 有如下的生成元

1) $\left[\begin{pmatrix}A & B\\ C & D\end{pmatrix}, I\right]\in O_{2\nu+2}(\mathbb{F}_q)$, 这里 $\begin{pmatrix}A & B\\ C & D\end{pmatrix}\in O_{2\nu}(\mathbb{F}_q)$.

2) $[I, I, U]\in O_{2\nu+2}(\mathbb{F}_q)$, 这里 $U\in O_2^-(\mathbb{F}_q)$.

3) $\left[\begin{pmatrix}J & I-J\\ I-J & J\end{pmatrix}, I\right]\in O_{2\nu+2}(\mathbb{F}_q)$, 这里 $J^2=J$ 为对角矩阵.

4) $\begin{pmatrix}I & P\Delta{}^tP & P\\ & I & \\ & (\Delta+{}^t\Delta){}^tP & I\end{pmatrix}$, $\begin{pmatrix}I & & \\ P\Delta{}^tP & I & P\\ (\Delta+{}^t\Delta){}^tP & & I\end{pmatrix}\in O_{2\nu+2}(\mathbb{F}_q)$, 这里 P 为 $\nu\times 2$ 的矩阵. 容易验证:

$$\left[\begin{pmatrix}{}^tA & {}^tC\\ {}^tB & {}^tD\end{pmatrix}, {}^tU\right]\left[\begin{pmatrix}0 & I\\ 0 & 0\end{pmatrix}, \Delta\right]\left[\begin{pmatrix}A & B\\ C & D\end{pmatrix}, U\right]\equiv\left[\begin{pmatrix}0 & I\\ 0 & 0\end{pmatrix}, \Delta\right];$$

$$\begin{pmatrix} I & X^t\Delta\,^tX & X(^t\Delta+\Delta) \\ & I & \\ & ^tX & I \end{pmatrix}\begin{pmatrix} 0 & I & \\ 0 & 0 & \\ & & \Delta \end{pmatrix}\begin{pmatrix} I & & \\ X\Delta\,^tX & I & X \\ (\Delta+\,^t\Delta)\,^tX & & I \end{pmatrix}$$

$$=\begin{pmatrix} 0 & I & X(\Delta+\,^t\Delta)\Delta \\ 0 & 0 & 0 \\ 0 & 0 & \Delta \end{pmatrix}\begin{pmatrix} I & & \\ X\Delta\,^tX & I & X \\ (\Delta+\,^t\Delta)\,^tX & & I \end{pmatrix}$$

$$=\begin{pmatrix} X\Delta\,^tX+X(\Delta+\,^t\Delta)\Delta(\Delta+\,^t\Delta)\,^tX & I & X+X(\Delta\,^t\Delta)\Delta \\ 0 & 0 & 0 \\ \Delta(\Delta+\,^t\Delta)\,^tX & 0 & \Delta \end{pmatrix}$$

$$\equiv\left[\begin{pmatrix} 0 & I \\ 0 & 0 \end{pmatrix},\Delta\right].$$

同理可证

$$\begin{pmatrix} I & & \\ Y\,^t\Delta\,^tY & I & Y(^t\Delta+\Delta) \\ ^tY & & I \end{pmatrix}\begin{pmatrix} 0 & I & \\ 0 & 0 & \\ & & \Delta \end{pmatrix}\begin{pmatrix} I & Y\Delta\,^tY & Y \\ & I & \\ & (\Delta+\,^t\Delta)\,^tY & I \end{pmatrix}$$

$$\equiv\left[\begin{pmatrix} 0 & I \\ 0 & 0 \end{pmatrix},\Delta\right],$$

$$\begin{pmatrix} J & I-J & \\ I-J & J & \\ & & I \end{pmatrix}\begin{pmatrix} 0 & I & \\ 0 & 0 & \\ & & \Delta \end{pmatrix}\begin{pmatrix} J & I-J & \\ I-J & J & \\ & & I \end{pmatrix}\equiv\begin{pmatrix} 0 & I & \\ 0 & 0 & \\ & & \Delta \end{pmatrix}.$$

所以

$$T\in O_{2\nu+2}(\mathbb{F}_q)\Longleftrightarrow\,^tT\in O_{2\nu+2}(\mathbb{F}_q).\qquad\square$$

我们定义 $O_{2\nu+\delta}(\mathbb{F}_q)$ 在 $\mathbb{F}_q^{(2\nu+\delta)}$ 上的作用如下

$$\begin{aligned}\mathbb{F}_q^{(2\nu+\delta)}\times O_{2\nu+\delta}(\mathbb{F}_q)&\longrightarrow\mathbb{F}_q^{(2\nu+\delta)}\\ ((x_1,x_2,\cdots,x_{2\nu+\delta}),T)&\longmapsto(x_1,x_2,\cdots,x_{2\nu+\delta})T.\end{aligned}$$

那么, 向量空间 $\mathbb{F}_q^{(2\nu+\delta)}$ 连同上面所定义的作用被称为 $\mathbb{F}_q$ 上关于 $G_{2\nu+\delta}$ 的 $2\nu+\delta$ 维正交空间.

我们知道, $\mathbb{F}_q$ 上 $m\times m$ 矩阵在“合同”意义下有三类标准型, 即

$$M(m,\,2s,\,s)\;=\left[\begin{pmatrix}0 & I^{(s)}\\ & 0\end{pmatrix},\,0^{(m-2s)}\right],$$

$$M(m,\,2s+1,\,s)\;=\left[\begin{pmatrix}0 & I^{(s)}\\ & 0\end{pmatrix},\,1,\,0^{(m-2s-1)}\right],$$

$$M(m,\,2s+2,\,s)\;=\left[\begin{pmatrix}0 & I^{(s)}\\ & 0\end{pmatrix},\,\begin{pmatrix}\alpha & 1\\ & \alpha\end{pmatrix},\,0^{(m-2s-2)}\right].$$

我们用 $M(m,\,2s+\gamma,\,s)(\gamma=0,1,2)$ 泛指上述三种情形.

令 P 是 $\mathbb{F}_q{}^{(2\nu+\delta)}$ 的一个 m 维子空间, 它的矩阵表示也记作 P. 这样, P 为一个秩为 m 的 $m\times(2\nu+\delta)$ 矩阵. 如果 $PG\,{}^tP$ “合同” 于 $M(m,\,2s+\gamma,\,s)$, 那么 P 被称为$(m,\,2s+\gamma,\,s,\,\Gamma)$ 型子空间, 这里 Γ 仅在 $\delta=\gamma=1$ 时出现, 而且 $e_{2\nu+1}\in P,\,\Gamma=1$; 否则, $\Gamma=0$. 两个 m 维子空间 P_1 和 P_2 有相同的类型, 当且仅当存在 $T\in O_{2\nu+\delta}(\mathbb{F}_q)$ 使得 $P_1=AP_2T$, 这里 $A\in GL_m(\mathbb{F}_q)$. 换句话说, 正交空间 $\mathbb{F}_q^{(2\nu+\delta)}$ 中具有相同类型的子空间作成 $O_{2\nu+\delta}(\mathbb{F}_q)$ 作用下的轨道. 令 $N(m,2s+\gamma,s,\Gamma;2\nu+\delta)$ 表示 $\mathbb{F}_q^{(2\nu+\delta)}$ 中型为 $(m,2s+\gamma,s,\Gamma)$ 的子空间的个数.[15] 的定理 7.28 给出如下计数公式:

$$N(m,2s+\gamma,s,\Gamma;2\nu+\delta)=q^{2s(\nu+s-m)+s(\delta+\gamma)-\gamma(m-2s-\gamma)}\cdot\frac{\displaystyle\prod_{i=\nu+s-m+\gamma-1}^{\nu}(q^i-1)(q^{i+\delta-1}+1)}{\displaystyle\prod_{i=1}^{s}(q^i-1)\prod_{i=0}^{s+\gamma-1}(q^i+1)\prod_{i=1}^{m-2s-\gamma}(q^i-1)}\cdot n_0(m,2s+\gamma,s,\Gamma;2\nu+\delta),\tag{7.7}$$

这里 $n_0(m,\,2s,\,s;\,2\nu+\delta)=1$;

$$n_0(m,2s+1,s,\Gamma;2\nu+\delta)=\begin{cases}2q^{\nu-s-1}(q^{\nu+s-m+1}-1), & \text{如果}\,\delta=0,\\ 2q^{m-2s-1}(q^{2(\nu+s-m+1)}-1), & \text{如果}\,\delta=1,\Gamma=0,\\ 2q^{m-2s-1}, & \text{如果}\,\delta=1,\Gamma=1,\\ 2q^{\nu-s}(q^{\nu+s-m+2}+1), & \text{如果}\,\delta=2;\end{cases}$$

$$n_0(m,2s+2,s;2\nu+\delta)=\begin{cases}q^{2(\nu-s)-2}(q^{\nu+s-m+1}-1)(q^{\nu+s-m+2}-1), & \text{如果}\,\delta=0,\\ q^{2(\nu-s)-1}(q^{\nu+s-m+2}-1)(q^{\nu+s-m+2}+1), & \text{如果}\,\delta=1,\\ q^{2(\nu-s)}(q^{\nu+s-m+2}+1)(q^{\nu+s-m+3}+1), & \text{如果}\,\delta=2.\end{cases}$$

还应指出, $(m,\,2s+\gamma,\,s,\,\Gamma)$ 型子空间存在的条件是

$$2s+\gamma\leqslant m\leqslant\begin{cases}\nu+s+\min\{\delta,\gamma\}, & \text{如果}\,\delta\neq1,\text{或}\,\gamma\neq1,\text{或}\,\delta=\gamma=1\,\text{且}\,\Gamma=1,\\ \nu+s+\gamma-1, & \text{如果}\,\delta=\gamma=1\,\text{而}\,\Gamma=0.\end{cases}\tag{7.8}$$

我们用 $n(m,\, 2s+\gamma,\, s,\, \Gamma;\, 2\nu+\delta)$ 表示 $\mathbb{F}_q^{(2\nu+\delta)}$ 中 $(m,\, 2s+\gamma,\, s,\, \Gamma)$ 型子空间的表示矩阵的个数. 由于我们在下面关于结合方案 Qua$(n,\, q)$ 的参数计算采取了一种逐次降阶的方法 (不同于前面几章中的算法), 主要应用 (7.7) 中 $m=1$ 时的如下计数公式:

(a) $n(1,\, 0,\, 0;\, 2\nu+\delta)=(q^2-1)(q^{\nu+\delta-1}+1)\quad(\nu\geqslant1)$, (7.9)

$$\text{(b)}\ n(1,\, 1,\, 0,\, \Gamma;\, 2\nu+\delta)=\begin{cases}q^{\nu}(q^{\nu}-1), & \text{如果},\delta=0,\\ (q^{2\nu}-1), & \text{如果}\,\delta=1,\Gamma=0,\\ 1, & \text{如果}\,\delta=1,\Gamma=1,\\ q^{\nu}(q^{\nu+1}+1), & \text{如果}\,\delta=2,\end{cases}\tag{7.10}$$

这里

$$\nu\geqslant\begin{cases}1, & \text{如果}\,\delta=0,\text{或}\,\delta=1\,\text{而}\,\Gamma=0,\\ 0, & \text{如果}\,\delta=2,\,\text{或}\,\delta=1\,\text{而}\,\Gamma=1.\end{cases}$$

(a) 和 (b) 分别是正交空间 $\mathbb{F}_q^{(2\nu+\delta)}$ 中的非零奇异向量和非奇异向量的计数公式.

关于正交群 $O_{2\nu+\delta}(\mathbb{F}_q)$ 的阶, 由 [15] 的定理 7.23 知

$$|O_{2\nu+\delta}(\mathbb{F}_q)|=\begin{cases}q^{\nu(\nu+\delta-1)}\prod_{i=1}^{\nu}(q^i-1)\prod_{i=0}^{\nu+\delta-1}(q^i+1), & \text{如果}\,\delta=0\,\text{或}\,2,\\ q^{\nu^2}\prod_{i=1}^{\nu}(q^{2i}-1), & \text{如果}\,\delta=1.\end{cases}\tag{7.11}$$

利用它我们很容易给出 $\mathbb{F}_q$ 上具有相同类型的 n 元二次型的计数公式. 令 $Q_i(n,q)$ 表示 $Q(n,q)$ 中类型为 i 的二次型的集合, $i\in\{0,1,2^+,2^-,\cdots\}$. 设 $i=(2s+\gamma,s)$, 那么 $Q_{(2s+\gamma,s)}(n,q)$ 就是 $GL_n(\mathbb{F}_q)$ 作用在 $Q(n,q)$ 上 (即"合同"变换) 二次型 $M(n,2s+\gamma,s)$ 所在的轨道. 于是有

$$|Q_{(2s+\gamma,s)}(n,q)|=|GL_n(\mathbb{F}_q)|/|H|,\tag{7.12}$$

这里 H 为 $M(n,2s+\gamma,s)$ 在 $GL_n(\mathbb{F}_q)$ 中的稳定子, 它由 $GL_n(\mathbb{F}_q)$ 中满足条件

$$TM(n,2s+\gamma,s)\,{}^tT\equiv M(n,2s+\gamma,s)$$

的矩阵 T 组成. 将 T 相应于 $M(n,2s+\gamma,s)$ 分块

$$T=\begin{pmatrix}A & B\\ C & D\end{pmatrix},$$

这里 A, D 分别为 $2s+\gamma, n-2s-\gamma$ 阶方阵. 这样就有下面的等式

$$AG_{2s+\gamma}{}^tA \equiv G_{2s+\gamma},\ A(G_{2s+\gamma}+{}^tG_{2s+\gamma}){}^tC=0,\ CG_{2s+\gamma}{}^tC\equiv 0.$$

于是 $A\in O_{2s+\gamma}(\mathbb{F}_q)$, 因而 A 非奇异. 由第二个等式得 $(G_{2s+\gamma}+{}^tG_{2s+\gamma}){}^tC=0$. 如果 $\gamma=0$ 或 2, 立得 $C=0$. 如果 $\gamma=1$, 则推出 C 的前 $2s+\gamma-1$ 列均为 0. 再由第三个式子可得 $C=0$. 这样, D 非奇异, B 为任意 $(2s+\gamma)\times(n-2s-\gamma)$ 矩阵. 因而

$$|H|=|O_{2s+\gamma}(\mathbb{F}_q)||GL_{n-2s-\gamma}(\mathbb{F}_q)|q^{(2s+\gamma)(n-2s-\gamma)}. \tag{7.13}$$

由 (7.11), (7.12) 和 (7.13), 我们有

定理 7.8 $\mathbb{F}_q$ 上型为 $(2s+\gamma,s)$ 的 n 元二次型的个数

$$|Q_{(2s+\gamma,s)}(n,q)|=\begin{cases} q^{s(s+\gamma)+\frac{1}{2}\gamma(\gamma-1)}\dfrac{\prod\limits_{j=s+1}^{n}(q^j-1)}{\prod\limits_{j=0}^{s+\gamma-1}(q^j+1)\prod\limits_{j=1}^{n-2s-\gamma}(q^j-1)}, & \text{如果}\gamma=0\text{或}2,\\ q^{s(s+1)}\dfrac{\prod\limits_{j=s+1}^{n}(q^j-1)}{\prod\limits_{j=1}^{s}(q^j+1)\prod\limits_{j=1}^{n-2s-1}(q^j-1)}, & \text{如果}\gamma=1.\end{cases}$$

§7.4 二次型结合方案的参数计算

在这一节中，我们讨论 $\mathbb{F}_q$ 上 n 元二次型结合方案 $\mathrm{Qua}(n,q)$ 的参数计算. 它的基础集合为 $Q(n,q)$, 其元素个数

$$|Q(n,q)|=q^{\frac{1}{2}n(n+1)}. \tag{7.14}$$

$\mathrm{Qua}(n,q)$ 的非平凡结合类的个数 $d=n+[\frac{n}{2}]$. 结合类 R_i 由 $Q(n,q)$ 的"合同"类 $Q_i(n,q)$ 所确定, R_i 的价 $k_i(n)=|Q_i(n,q)|$, 这里 i 表示二次型的类型. 在后面的讨论中，我们把类型 $i=(2s+\gamma,s)$ 简记为 $i=2s+\gamma$, $\gamma=0,1$ 或 2. 这样，由定理 7.8 知，结合关系 $R_{2s+\gamma}$ 的价为

$$k_{2s+\gamma}(n)=q^{s(s+\gamma)+\frac{1}{2}\gamma(\gamma-1)}\frac{\prod\limits_{j=s+1}^{n}(q^j-1)}{\prod\limits_{j=\frac{1}{2}[1-(-1)^\gamma]}^{s+\gamma-1}(q^j+1)\prod\limits_{j=1}^{n-2s-\gamma}(q^j-1)}. \tag{7.15}$$

如果 $\gamma=0$, 类型 $i=2s$ 也记作 $i=2s^+$; 如果 $\gamma=2$, 类型 $i=2s+2$ 也记作 $i=2s+2^-$ 或者 $i=2(s+1)^-$. 设二次型 $A=[A_1,A_2]$, 简单计算可知 A 的类型由 A_1 和 A_2 的类型唯一确定，它们的类型之间的关系由表 7.1 给出

表 7.1　A 与 A_1, A_2 类型之间的关系

A_1 / A / A_2	$2j_1^+$	$2j_1+1$	$2j_1+2^-$
$2j_2^+$	$2(j_1+j_2)^+$	$2(j_1+j_2)+1$	$2(j_1+j_2)+2^-$
$2j_2+1$	$2(j_1+j_2)+1$	$2(j_1+j_2)+1$	$2(j_1+j_2+1)+1$
$2j_2+2^-$	$2(j_1+j_2)+2^-$	$2(j_1+j_2+1)+1$	$2(j_1+j_2+2)^+$

我们仅以 A_1 和 A_2 的类型分别为 $2j_1+2^-$ 和 $2j_2+2^-$ 为例给以证明.

由 $A_i(i=1,2)$ 的类型可知, 存在 $T_i \in GL_{n_i}(F_q)(i=1,2)$ 使得

$$T_iA_i{}^tT_i \equiv \left[\begin{pmatrix} 0 & I^{(j_i)} \\ & 0 \end{pmatrix}, \begin{pmatrix} \alpha & 1 \\ & \alpha \end{pmatrix}, 0^{(m_i)}\right], m_i = n_i - 2j_i - 2.$$

容易看出

$$\begin{pmatrix} \alpha & 1 & & \\ & \alpha & & \\ & & \alpha & 1 \\ & & & \alpha \end{pmatrix} \sim \begin{pmatrix} 0 & & 1 & \\ & 0 & & 1 \\ & & 0 & \\ & & & 0 \end{pmatrix},$$

所以结论成立.

现在要给出关于一般参数 $p^{2j_1+\delta_1}_{2j_2+\delta_2\ 2j_3+\delta_3}(n)$ 的一组递推计算公式.

令 $H_0 = 0$, H_1 是一个类型为 $2j_1+\delta_1$ 的矩阵, 并令

$$M = \{H \in Q(n,q) | t(H) = 2j_2+\delta_2, t(H-H_1) = 2j_3+\delta_3\}.$$

那么

$$p^{2j_1+\delta_1}_{2j_2+\delta_2\ 2j_3+\delta_3}(n) = |M|.$$

为了计算 $p^{2j_1+\delta_1}_{2j_2+\delta_2\ 2j_3+\delta_3}(n)$, 不妨取定

$$H_1 = \left[\begin{pmatrix} 0 & I^{(j_1)} \\ & 0 \end{pmatrix}, \Delta_1, 0^{(m)}, 0\right],$$

这里 $m = n - 2j_1 - \delta_1 - 1$. 设 $H = \begin{pmatrix} A & V \\ 0 & u \end{pmatrix}$, 其中 A 是一个 $(n-1)\times(n-1)$ 矩阵, V 是一个 $n-1$ 维列向量, $u \in \mathbb{F}_q$. 我们区分 $2j_1+\delta_1 < n$ 和 $2j_1+\delta_1 = n$ 两种情形讨论之.

(I) $2j_1+\delta_1 < n$.

令

$$Z = \left[\begin{pmatrix} 0 & I^{(j_1)} \\ & 0 \end{pmatrix}, \Delta_1, 0^{(m)}\right],$$

那么

$$H_1=\begin{pmatrix} Z & \\ & 0 \end{pmatrix},\quad H-H_1=\begin{pmatrix} A-Z & V \\ 0 & u \end{pmatrix}.$$

我们再区分 $V=0$ 和 $V\neq 0$ 两种情形.

(I-i) $V=0$.

如果 $u=0$, 那么

$$H=\begin{pmatrix} A & \\ & 0 \end{pmatrix},\quad H-H_1=\begin{pmatrix} A-Z & \\ & 0 \end{pmatrix}.$$

易知 M 中这种形状的 H 个数为

$$p^{2j_1+\delta_1}_{2j_2+\delta_2\ 2j_3+\delta_3}(n-1). \tag{7.16}$$

如果 $u\neq 0$, 易见 $\delta_2=\delta_3=1$. 这时

$$H=\begin{pmatrix} A & \\ & u \end{pmatrix},\quad H-H_1=\begin{pmatrix} A-Z & \\ & u \end{pmatrix}.$$

这样 A 的型可能为 $2j_2^+, 2j_2+1$ 或 $2(j_2-1)+2^-$. $A-Z$ 的型可能为 $2j_3^+, 2j_3+1$ 或 $2(j_3-1)+2^-$. 因此, M 中如此形状的 H 个数为

$$(q-1)\sum_{l,k}^{n-1} p^{2j_1+\delta_1}_{lk}(n-1), \tag{7.17}$$

这里 $l\in\{2j_2^+, 2j_2+1, 2(j_2-1)+2^-\}$, $k\in\{2j_3^+, 2j_3+1, 2(j_3-1)+2^-\}$.

(I-ii) $V\neq 0$.

设 $V={}^t(v_1, v_2, \cdots, v_{n-1})$,

$$G=\left[\begin{pmatrix} 0 & I^{(j_1)} \\ & 0 \end{pmatrix}, \Delta_1\right], H_1=\left[G, 0^{(m)}, 0\right], H=\begin{pmatrix} A & B & V_1 \\ & C & V_2 \\ & & u \end{pmatrix}, \tag{7.18}$$

这里 H 写为与 H_1 相对应的分块形状. 我们又分以下两种情形.

(I-ii-1) $V_2\neq 0$.

这时 $m>0$. 令

$$S=\{H\in M | H \text{ 形如 } (7.18) \text{ 而 } V_2\neq 0\}.$$

因为 $V_2\neq 0$, 存在矩阵 $T\in GL_m(\mathbb{F}_q)$ 使得 $TV_2={}^t(0,\cdots,1)$. 设

$$T_1=\left[I^{(2j_1+\delta_1)}, T, 1\right], T_2=\left[\begin{pmatrix} I^{(2j_1+\delta_1)} & & V_1 \\ & I^{(m-1)} & \\ & & 1 \end{pmatrix}, 1\right].$$

那么, 在 T_1 和 T_2 的"合同"变换之下 H_1 保持不变, 而 H"合同"于矩阵

$$\begin{pmatrix} U & W & 0 \\ & a & 1 \\ & & u \end{pmatrix}.$$

我们把 S 中所有如此形状的矩阵的集合记作 S_1, 那么

$$|S| = (q^{n-1} - q^{2j_1+\delta_1})|S_1|. \tag{7.19}$$

再令

$$T_3 = \begin{pmatrix} I^{(n-2)} & & W \\ & 1 & \\ & & 1 \end{pmatrix},$$

那么在 T_3 的"合同"变换之下, H_1 保持不变, S_1 中的 H 变成

$$\begin{pmatrix} U_1 & \\ & D \end{pmatrix}, \text{这里 } D = \begin{pmatrix} a & 1 \\ & u \end{pmatrix}.$$

我们用 S_2 表示 S_1 中如此形状矩阵所成的集合. 那么

$$|S_1| = q^{n-2}|S_2|, \tag{7.20}$$

而 $t(D) = 2^+$ 或 2^-.

如果 $t(D) = 2^+$, 那么

$$|S_2| = \frac{1}{2}q(q+1)p^{2j_1+\delta_1}_{2(j_2-1)+\delta_2\ 2(j_3-1)+\delta_3}(n-2) \tag{7.21}$$

如果 $t(D) = 2^-$, 那么

$$|S_2| = \frac{1}{2}q(q-1)p^{2j_1+\delta_1}_{2(j_2-2+\delta_2)+(2-\delta_2)\ 2(j_3-2+\delta_3)+(2-\delta_3)}(n-2). \tag{7.22}$$

综合 (7.19)~(7.22) 式, 得到

$$\begin{aligned} |S| = & \frac{1}{2}q^{n-1}(q^{n-1} - q^{2j_1+\delta_1})[(q+1)p^{2j_1+\delta_1}_{2(j_2-1)+\delta_2\ 2(j_3-1)+\delta_3}(n-2) \\ & +(q-1)p^{2j_1+\delta_1}_{2(j_2-2+\delta_2)+(2-\delta_2)\ 2(j_3-2+\delta_3)+(2-\delta_3)}(n-2)]. \end{aligned} \tag{7.23}$$

(I-ii-2) $V_2 = 0$ 或不出现, 而 $V_1 \neq 0$.

我们先讨论 $\delta_1 = 0$ 或 2 的情形, 这时 $n \geqslant 3$. 令

$$C = \{H \in M | H \text{ 形如 } (7.18), \text{而 } V_1 \neq 0, V_2 = 0\}.$$

我们再分 ${}^tV_1GV_1=0$ 和 ${}^tV_1GV_1\neq 0$ 两种情形.

(I-ii-2.a) ${}^tV_1GV_1=0$.

令 $C^{(a)}=\{H\in C|{}^tV_1GV_1=0\}$. 根据定理 7.7 和同型子空间的可迁性, 存在 $T^*\in O_{2j_1+\delta_1}(\mathbb{F}_q)$ 使得 $T^*V_1={}^t(1,0,\cdots,0)$. 设

$$T_1^*=\left[T^*,I^{(m)},1\right],\quad T_4=\left[\begin{pmatrix}0 & & 1\\ & I^{(n-3)} & \\ 1 & & 0\end{pmatrix},1\right].$$

(这里引入 T_4, 目的在于讨论中矩阵形状便于书写). 于是

当 $n>2j_1+\delta_1+1$ 时,

$${}^tT_4\,{}^t(T_1^*)H_1T_1^*T_4\equiv\left[\begin{pmatrix}\begin{pmatrix}G+E_{1j_1+1} & \\ & 0^{(m-1)}\end{pmatrix} & e_{j_1+1}\\ & 0\end{pmatrix},0\right]. \tag{7.24}$$

当 $n=2j_1+\delta_1+1$ 时

$${}^tT_4\,{}^t(T_1^*)H_1T_1^*T_4\equiv\begin{cases}[G_0+E_{1j_1}+E_{j_1+1\,2j_1}+E_{1j_1+1}+E_{j_12j_1},0],\\ \quad\text{如果 }\delta_1=0,\ n=2j_1+1,\\ \left[\begin{pmatrix}G_0+\alpha E_{11}+E_{1j_1+1} & e_1 & e_{j_1+1}\\ & \alpha & \\ & & 0\end{pmatrix},0\right],\\ \quad\text{如果 }\delta_1=2,\ n=2j_1+3,\end{cases} \tag{7.25}$$

这里

$$G_0=\begin{pmatrix}0 & I^{(j_1)}\\ & 0\end{pmatrix},$$

E_{ij} 为 (i,j) 位置元素为 1, 其他位置元素皆为 0 的矩阵;e_i 是第 i 个位置元素为 1, 其他位置元素皆为 0 的 $2j_1+\delta_1-$ 维列向量. 在此变换下, H“合同” 于

$$\begin{pmatrix}U & W & 0\\ & a & 1\\ & & u\end{pmatrix}.$$

我们把 C 中所有如此形状的矩阵的集合记作 $C_1^{(a)}$, 那么

$$|C^{(a)}|=n(1,0,0,2j_1+\delta_1)|C_1^{(a)}|. \tag{7.26}$$

因为在 “合同” 变换 T_3 下, ${}^tT_4\,{}^t(T_1^*)H_1T_1^*T_4$ 不变, 而 $C_1^{(a)}$ 中的矩阵 H 则相应地 “合同” 于 $\begin{pmatrix}U_1 & \\ & D\end{pmatrix}$, $D=\begin{pmatrix}a & 1\\ & u\end{pmatrix}$. 我们用 $C_2^{(a)}$ 表示 $C_1^{(a)}$ 中如此形状矩阵的集合, 那么

$$|C_1^{(a)}| = q^{n-2}|C_2^{(a)}|. \tag{7.27}$$

对于 $H \in C_2^{(a)}$, 当 $n > 2j_1 + \delta_1 + 1$ 时,

$$H - H_1 \sim \begin{pmatrix} \begin{pmatrix} G + E_{1j_1+1} & \\ & 0^{(m-1)} \end{pmatrix} + U_1 & (e_{j_1+1} \quad 0) \\ & D \end{pmatrix}$$

$$\sim \begin{pmatrix} \begin{pmatrix} G + E_{1j_1+1} + uE_{j_1+1j_1+1} & \\ & 0^{(m-1)} \end{pmatrix} + U_1 & \\ & D \end{pmatrix}.$$

因为 $t(H) = 2j_2 + \delta_2$, $t(H - H_1) = 2j_3 + \delta_3$, 所以 U_1 的取法随 D 的类型和 u 的值所确定. 于是对应于 D 的可能的类型和 u 的不同的值, 下面给出 $C_2^{(a)}$ 中适合各种可能的不同条件的元素个数.

(1) 如果 $t(D) = 2^+$, $u = 0$, 那么在 $C_2^{(a)}$ 中元素的个数是

$$qp^{2(j_1-1)+\delta_1}_{2(j_2-1)+\delta_2 \ 2(j_3-1)+\delta_3}(n-2); \tag{7.28}$$

(2) 如果 $t(D) = 2^+$, $u \neq 0$, 那么在 $C_2^{(a)}$ 中元素的个数是

$$\frac{1}{2}q(q-1)p^{2(j_1-1+\frac{1}{2}\delta_1)+1}_{2(j_2-1)+\delta_2 \ 2(j_3-1)+\delta_3}(n-2); \tag{7.29}$$

(3) 如果 $t(D) = 2^-$, $u \neq 0$, 那么在 $C_2^{(a)}$ 中元素的个数是

$$\frac{1}{2}q(q-1)p^{2(j_1-1+\frac{1}{2}\delta_1)+1}_{2(j_2-2+\delta_2)+(2-\delta_2) \ 2(j_3-2+\delta_3)+(2-\delta_3)}(n-2). \tag{7.30}$$

综合 (7.26)~(7.30) 式, 得到

$$\begin{aligned} |C^{(a)}| = & \frac{1}{2}q^{n-1}n(1, 0, 0, 2j_1 + \delta_1) \\ & \cdot [2p^{2(j_1-1)+\delta_1}_{2(j_2-1)+\delta_2 \ 2(j_3-1)+\delta_3}(n-2) \\ & + (q-1)p^{2(j_1-1+\frac{1}{2}\delta_1)+1}_{2(j_2-1)+\delta_2 \ 2(j_3-1)+\delta_3}(n-2) \\ & + (q-1)p^{2(j_1-1+\frac{1}{2}\delta_1)+1}_{2(j_2-2+\delta_2)+(2-\delta_2) \ 2(j_3-2+\delta_3)+(2-\delta_3)}(n-2)]. \end{aligned} \tag{7.31}$$

当 $n = 2j_1 + \delta_1 + 1$ 时, 可用类似的方法, 分别考虑 $\delta_1 = 0$, $n = 2j_1 + 1$; $\delta_1 = 2$, $n = 2j_1 + 3$ 两种情形, 也得到了同一表达式 (7.31).

(I-ii-2.b) ${}^tV_1GV_1 \neq 0$.

令 $C^{(b)} = \{H \in C | {}^tV_1GV_1 \neq 0\}$. 由定理 7.7 和同型子空间的可迁性, 存在 $T^\diamond \in O_{2j_1+\delta_1}(\mathbb{F}_q)$, 使得 $T^\diamond V_1 = {}^t(1, 0, \cdots, 0, 1, 0, \cdots, 0)$. 令

$$T_1^\diamond = [T^\diamond, I^{(m)}, 1].$$

对于 H_1, 我们有与情形 (I-ii-2.a) 相同的变换结果, 即当 $n > 2j_1 + \delta_1 + 1$ 时, ${}^tT_4{}^tT_1^\diamond H_1 T_1^\diamond T_4 \equiv$ (7.24) 同余号的右边; 当 $n = 2j_1 + \delta_1 + 1$ 时, ${}^tT_4{}^tT_1^\diamond H_1 T_1^\diamond T_4 \equiv$ (7.26) 同余号的右边. 在此变换下 H "合同" 于

$$\begin{pmatrix} \widetilde{U} & \widetilde{W} & e_{j_1+1} \\ & a & 1 \\ & & u \end{pmatrix}.$$

我们将 $C^{(b)}$ 中所有如此形状的二次型的集合记作 $C_1^{(b)}$, 那么

$$|C^{(b)}| = (q-1)n(1,1,0,2j_1+\delta_1)|C_1^{(b)}|. \tag{7.32}$$

令

$$T_5 = \left[I^{(j_1)}, \begin{pmatrix} 1 & & 1 \\ & I^{(n-j_1-3)} & \\ & & 1 \end{pmatrix}, 1 \right].$$

如果 $n > 2j_1 + \delta_1 + 1$, 那么在 "合同" 变换 T_5 之下, ${}^tT_4\,{}^t(T_1^\diamond)H_1T_1^\diamond T_4$ 和 $C_1^{(b)}$ 中的 H 分别 "合同" 于

$$\widetilde{H_1} = \left[\left(\begin{pmatrix} G + E_{1j_1+1} + E_{j_1+1j_1+1} & \\ & 0^{(m-1)} \end{pmatrix} \begin{matrix} e_{j_1+1} \\ 0 \end{matrix} \right), 0 \right]$$

和

$$\begin{pmatrix} U & W & \\ & a & 1 \\ & & u \end{pmatrix}.$$

易见 $\widetilde{H_1}$ 在 "合同" 变换 T_3 之下不变, H 相应地 "合同" 于

$$\begin{pmatrix} U_1 & \\ & D \end{pmatrix}, \qquad \text{其中 } D = \begin{pmatrix} a & 1 \\ & u \end{pmatrix}.$$

我们用 $C_2^{(b)}$ 表示 $C_1^{(b)}$ 中如此形状矩阵的集合, 那么

$$|C_1^{(b)}| = q^{n-2}|C_2^{(b)}|. \tag{7.33}$$

进一步, 我们有

$$H - H_1 \sim \left[\begin{pmatrix} G + E_{1j_1+1} + (1+u)E_{j_1+1j_1+1} & \\ & 0^{(m-1)} \end{pmatrix} + U_1, D \right].$$

类似于情形 (I-ii-2.a) 的讨论, 下面对应于 D 可能有的类型和 u 的不同值, 给出 $C_2^{(b)}$ 中适合各种条件元素的个数.

(1) 如果 $t(D)=2^+$, $u=1$, 那么 $C_2^{(b)}$ 中元素的个数是

$$\frac{1}{2}qp_{2(j_2-1)+\delta_2 2(j_3-1)+\delta_3}^{2(j_1-1)+\delta_1}(n-2). \tag{7.34}$$

(2) 如果 $t(D)=2^+, u\neq 1$, 那么 $C_2^{(b)}$ 中元素的个数是

$$\frac{1}{2}q^2p_{2(j_2-1)+\delta_2 2(j_3-1)+\delta_3}^{2(j_1-1+\frac{1}{2}\delta_1)+1}(n-2). \tag{7.35}$$

(3) 如果 $t(D)=2^-$, $u=1$, 那么 $C_2^{(b)}$ 中元素的个数是

$$\frac{1}{2}qp_{2(j_2-2+\delta_2)+(2-\delta_2)2(j_3-2+\delta_3)+(2-\delta_3)}^{2(j_1-1)+\delta_1}(n-2). \tag{7.36}$$

(4) 如果 $t(D)=2^-$, $u\neq 0,1$, 那么 $C_2^{(b)}$ 中元素的个数是

$$\frac{1}{2}q(q-2)p_{2(j_2-2+\delta_2)+(2-\delta_2)2(j_3-2+\delta_3)+(2-\delta_3)}^{2(j_1-1+\frac{1}{2}\delta_1)+1}(n-2). \tag{7.37}$$

综合 (7.32)~(7.37) 式, 得到

$$\begin{aligned}|C^{(b)}|=&\frac{1}{2}q^{n-1}(q-1)n(1,\,1,\,0,\,2j_1+\delta_1)\\&\cdot[p_{2(j_2-1)+\delta_2 2(j_3-1)+\delta_3}^{2(j_1-1)+\delta_1}(n-2)\\&+qp_{2(j_2-1)+\delta_2 2(j_3-1)+\delta_3}^{2(j_1-1+\frac{1}{2}\delta_1)+1}(n-2)\\&+p_{2(j_2-2+\delta_2)+(2-\delta_2)2(j_3-2+\delta_3)+(2-\delta_3)}^{2(j_1-1)+\delta_1}(n-2)\\&+(q-2)p_{2(j_2-2+\delta_2)+(2-\delta_2)2(j_3-2+\delta_3)+(2-\delta_3)}^{2(j_1-1+\frac{1}{2}\delta_1)+1}(n-2)],\end{aligned} \tag{7.38}$$

当 $n=2j_1+\delta_1+1$ 时, 用类似的方法, 分别考虑 $\delta_1=0$, $n=2j_1+1$; $\delta_1=2$, $n=2j_1+3$ 两种情形, 也得到了同一表达式 (7.38). 因此

$$|C|=|C^{(a)}|+|C^{(b)}|. \tag{7.39}$$

综合以上情形 (I-i), (I-ii-1), (I-ii-2), 由 (7.16), (7.17), (7.26), (7.31), (7.38) 和 (7.39) 式, 就得如下

定理 7.9 对于 $\delta_1=0$ 或 2, 我们有

$$\begin{aligned}&p_{2j_2+\delta_2 2j_3+\delta_3}^{2j_1+\delta_1}(n)\\=&p_{2j_2+\delta_2 2j_3+\delta_3}^{2j_1+\delta_1}(n-1)+f(\delta_2,\delta_3)(q-1)\sum_{l,k}p_{lk}^{2j_1+\delta_1}(n-1)\\&+\frac{1}{2}q^{n-1}(q^{j_1+\frac{\delta_1}{2}}+(-1)^{\frac{\delta_1}{2}+1})\end{aligned}$$

$$\cdot\{(q^{j_1+\frac{\delta_1}{2}}+q^{j_1+\frac{\delta_1}{2}-1}-(-1)^{\frac{\delta_1}{2}+1}2)\cdot p^{2(j_1-1)+\delta_1}_{2(j_2-1)+\delta_2 2(j_3-1)+\delta_3}(n-2)$$

$$+(q-1)q^{j_1+\frac{\delta_1}{2}-1}p^{2(j_1-1)+\delta_1}_{2(j_2-2+\delta_2)+(2-\delta_2)2(j_3-2+\delta_3)+(2-\delta_3)}(n-2)\}$$

$$+\frac{1}{2}q^{n-1}(q-1)(q^{j_1+\frac{\delta_1}{2}}+(-1)^{\frac{\delta_1}{2}+1})(q^{j_1+\frac{\delta_1}{2}}+q^{j_1+\frac{\delta_1}{2}-1}-(-1)^{\frac{\delta_1}{2}+1})$$

$$\cdot\{p^{2(j_1-1+\frac{1}{2}\delta_1)+1}_{2(j_2-1)+\delta_2 2(j_3-1)+\delta_3}(n-2)+p^{2(j_1-1+\frac{1}{2}\delta_1)+1}_{2(j_2-2+\delta_2)+(2-\delta_2)2(j_3-2+\delta_3)+(2-\delta_3)}(n-2)\}$$

$$+\frac{1}{2}q^{n-1}(q^{n-1}-q^{2j_1+\delta_1})\{(q+1)p^{2j_1+\delta_1}_{2(j_2-1)+\delta_2 2(j_3-1)+\delta_3}(n-2)$$

$$+(q-1)\cdot p^{2j_1+\delta_1}_{2(j_2-2+\delta_2)+(2-\delta_2)2(j_3-2+\delta_3)+(2-\delta_3)}(n-2)\},$$

这里 $l\in\{2j_2^+,\,2j_2+1,\,2(j_2-1)+2^-\}$, $k\in\{2j_3^+,\,2j_3+1,\,2(j_3-1)+2^-\}$; 而 $f(\delta_2,\delta_3)=1$, 如果 $\delta_2=\delta_3=1$; 否则 $f(\delta_2,\delta_3)=0$. □

现在讨论 (I-ii-2) 中 $\delta_1=1$ 的情形.

(I-ii-2′) $\delta_1=1$, $V_2=0$, $v_{2j_1+1}=0$.

设

$$C'=\{H\in M|H \text{ 形如 } (7.18), \text{ 而 } V_2=0,\ v_{2j_1+1}=0.$$

令 $V_0={}^t(v_1,\cdots,v_{2j_1})$, 考虑如下两种情形

(I-ii-2′.a) ${}^tV_0G_0V_0=0$.

令 $C'^{(a)}=\{H\in C'|{}^tV_0G_0V_0=0\}$, 这时存在 $\overline{T}\in O_{2j_1}(\mathbb{F}_q)$ 使得 $\overline{T}V_0={}^t(1,0,\cdots,0)$. 令

$$\overline{T_1}=[\overline{T},\,I^{(m+1)},\,1],$$

那么, 当 $n>2j_1+2$ 时,

$${}^tT_4\,{}^t(\overline{T_1})H_1\overline{T_1}T_4\equiv\left[\left(\begin{pmatrix}G+E_{1j_1+1} & \\ & 0^{(m-1)}\end{pmatrix}\begin{matrix}e_{j_1+1}\\0\end{matrix}\right),0\right].$$

当 $n=2j_1+2$ 时,

$${}^tT_4\,{}^t(\overline{T_1})H_1\overline{T_1}T_4\equiv\left[\begin{pmatrix}G_0+E_{1j_1+1}+E_{11} & e_{j_1+1}\\ & 0\end{pmatrix},0\right].$$

如同情形 (I-ii-2.a) 的讨论, 不再重复类似的计算过程, 仅列出结果如下

$$\begin{aligned}|C'^{(a)}|=&\frac{1}{2}q^{n-1}n(1,0,0,2j_1)[(q+1)p^{2(j_1-1)+1}_{2(j_2-1)+\delta_2 2(j_3-1)+\delta_3}(n-2)\\&+(q-1)p^{2(j_1-1)+1}_{2(j_2-2+\delta_2)+(2-\delta_2)2(j_3-2+\delta_3)+(2-\delta_3)}(n-2)]\end{aligned}\tag{7.40}$$

(I-ii-2′.b) ${}^tV_0G_0V_0\neq0$.

令 $C'^{(b)} = \{H \in C' | {}^tV_0G_0V_0 \neq 0\}$, 类似于情形 (II.2.b) 的讨论, 得到

$$\begin{aligned}|C'^{(b)}| = &\frac{1}{2}q^{n-1}(q-1)n(1,1,0,2j_1)\\ &\cdot[(q+1)p^{2(j_1-1)+1}_{2(j_2-1)+\delta_2 2(j_3-1)+\delta_3}(n-2)\\ &+(q-1)p^{2(j_1-1)+1}_{2(j_2-2+\delta_2)+(2-\delta_2)2(j_3-2+\delta_3)+(2-\delta_3)}(n-2)].\end{aligned} \tag{7.41}$$

于是

$$\begin{aligned}|C'| &= |C'^{(a)}| + |C'^{(b)}|\\ &= \frac{1}{2}q^{n-1}(q^{2j_1}-1)\{(q+1)p^{2(j_1-1)+1}_{2(j_2-1)+\delta_2 2(j_3-1)+\delta_3}(n-2)\\ &\quad +(q-1)p^{2(j_1-1)+1}_{2(j_2-2+\delta_2)+(2-\delta_2)2(j_3-2+\delta_3)+(2-\delta_3)}(n-2)\}.\end{aligned} \tag{7.42}$$

(I-ii-3) $\delta_1 = 1$, $V_2 = 0$, $v_{2j_1+1} \neq 0$.

设

$$L = \{H \in M | H \text{ 形如 } (7.18), \text{ 而 } V_2 = 0,\ v_{2j_1+1} \neq 0\}.$$

令

$$T_{4'} = \left[I^{(2j_1)}, \begin{pmatrix} 0 & & 1 \\ & I^{(n-2j_1-3)} & \\ 1 & & 0 \end{pmatrix}, 1\right].$$

那么

$${}^tT_{4'}H_1T_{4'} = \left[G_0, 0^{(n-2j_1-2)}, D_0\right],$$

这里 $D_0 = [1, 0]$, 而且在 "合同" 变换 $T_{4'}$ 之下, H "合同" 于

$$\widetilde{H} = \begin{pmatrix} U_1 & U_2 & W_1 & X \\ & U_3 & W_2 & 0 \\ & & a & v_{2j_1+1} \\ & & & u \end{pmatrix}.$$

再令

$$T_{3'} = \left[\begin{pmatrix} I^{(2j_1)} & & \\ & I^{(n-2j_1-2)} & \\ v^{-1}_{2j_1+1}X' & & 1 \end{pmatrix}, 1\right],$$

$$\widetilde{T_{3'}} = \begin{pmatrix} I^{(2j_1)} & & & \\ & I^{(n-2j_1-2)} & & \\ & & 1 & \\ v^{-1}_{2j_1+1}\,{}^tW_1 & v^{-1}_{2j_1+1}\,{}^tW_2 & & 1 \end{pmatrix}.$$

那么

$$ {}^t\widetilde{T_{3'}}\,{}^tT_{3'}\,{}^tT_{4'}H_1T_{4'}T_{3'}\widetilde{T_{3'}} \sim [Y,\ D_0] $$

和

$$ {}^t\widetilde{T_{3'}}\,{}^tT_{3'}\,{}^tT_{4'}HT_{4'}T_{3'}\widetilde{T_{3'}} \sim [U,\ D], $$

这里

$$ Y = \left[G_0 + v_{2j_1+1}^{-2}X\,{}^tX,\ 0^{(n-2j_1-2)}\right],\ D = \begin{pmatrix} a & v_{2j_1+1} \\ & u \end{pmatrix}. $$

我们再分 ${}^tXG_0X = 0$ 和 ${}^tXG_0X \neq 0$ 两种情形.

(I-ii-3.a) $X'G_0X = 0$. 由定理 7.7 和同型子空间的可迁性, 可以假设 $X\,{}^tX = E_{11}$ 或 $X = 0$. 因而对于 $t(Y) = 2j_1^+$, X 有 $n(1, 0, 0; 2j_1) + 1 = q^{j_1-1}(q^{j_1} + q - 1)$ 种取法; 而 W_1, W_2 的任意选取, 有 q^{n-2} 种取法; 依据 D 和 $D + D_0$ 的类型可能的不同取法, 下面给出 L 中适合条件的 H 的个数.

(1) 如果 $t(D) = 2^+$, $t(D + D_0) = 2^+$, 那么 L 中 H 的个数是

$$ \begin{aligned} &q^{n-2}q^{j_1-1}(q^{j_1} + q - 1) \\ &\cdot p^1_{2^+2^+}(2)p^{2j_1}_{2(j_2-1)+\delta_2 2(j_3-1)+\delta_3}(n-2). \end{aligned} \tag{7.43} $$

(2) 如果 $t(D) = 2^+$, $t(D + D_0) = 2^-$, 那么 L 中 H 的个数是

$$ \begin{aligned} &q^{n-2}q^{j_1-1}(q^{j_1} + q - 1) \\ &\cdot p^1_{2^+2^-}(2)p^{2j_1}_{2(j_2-1)+\delta_2 2(j_3-2+\delta_3)+(2-\delta_3)}(n-2). \end{aligned} \tag{7.44} $$

(3) 如果 $t(D) = 2^-$, $t(D + D_0) = 2^+$, 那么 L 中 H 的个数是

$$ \begin{aligned} &q^{n-2}q^{j_1-1}(q^{j_1} + q - 1) \\ &\cdot p^1_{2^-2^+}(2)p^{2j_1}_{2(j_2-2+\delta_2)+(2-\delta_2)2(j_3-1)+\delta_3}(n-2). \end{aligned} \tag{7.45} $$

(4) 如果 $t(D) = 2^-$, $t(D + D_0) = 2^-$, 那么 L 中 H 的个数是

$$ \begin{aligned} &q^{n-2}q^{j_1-1}(q^{j_1} + q - 1) \\ &\cdot p^1_{2^-2^-}(2)p^{2j_1}_{2(j_2-2+\delta_2)+(2-\delta_2)2(j_3-2+\delta_3)+(2-\delta_3)}(n-2). \end{aligned} \tag{7.46} $$

(I-ii-3.b) ${}^tXG_0X \neq 0$. 由定理 7.7 和同型子空间的可迁性, 不妨设 $X\,{}^tX = E_{11} + E_{j_1+1\,j_1+1}$. 因而 X 有 $(q-1)n(1, 1, 0; 2j_1) = (q-1)q^{j_1-1}(q^{j_1} - 1)$ 种取法, 而 W_1, W_2 的任取, 有 q^{n-2} 种取法. 根据 Y 不同的类型区分以下两种情形.

1) $v_{2j_1+1}^{-1} \in N$, 这时 $t(Y) = 2j_1^+$. 依据 D 和 D_0 的类型不同取法, 得到 L 中适合条件 (I-ii-2.b) 中情形 1) 的 H 的个数由下面给出

(1) 如果 $t(D)=2^+$, $t(D+D_0)=2^+$, 那么 L 中 H 的个数是

$$\begin{aligned}&\frac{1}{2}(q-2)q^{n-2}(q-1)q^{j_1-1}(q^{j_1}-1)\\&\cdot\frac{1}{4}q(q+2)p^{2j_1}_{2(j_2-1)+\delta_2\,2(j_3-1)+\delta_3}(n-2).\end{aligned}\tag{7.47}$$

(2) 如果 $t(D)=2^+$, $t(D+D_0)=2^-$, 那么 L 中 H 的个数是

$$\begin{aligned}&\frac{1}{2}(q-2)q^{n-2}(q-1)q^{j_1-1}(q^{j_1}-1)\\&\cdot\frac{1}{4}q^2p^{2j_1}_{2(j_2-1)+\delta_2\,2(j_3-2+\delta_3)+(2-\delta_3)}(n-2).\end{aligned}\tag{7.48}$$

(3) 如果 $t(D)=2^-$, $t(D+D_0)=2^+$, 那么 L 中 H 的个数是

$$\begin{aligned}&\frac{1}{2}(q-2)q^{n-2}(q-1)q^{j_1-1}(q^{j_1}-1)\\&\cdot\frac{1}{4}q^2p^{2j_1}_{2(j_2-2+\delta_2)+(2-\delta_2)2(j_3-1)+\delta_3}(n-2).\end{aligned}\tag{7.49}$$

(4) 如果 $t(D)=2^-$, $t(D+D_0)=2^-$, 那么 L 中 H 的个数是

$$\begin{aligned}&\frac{1}{2}(q-2)q^{n-2}(q-1)q^{j_1-1}(q^{j_1}-1)\\&\cdot\frac{1}{4}q(q-2)p^{2j_1}_{2(j_2-2+\delta_2)+(2-\delta_2)2(j_3-2+\delta_3)+(2-\delta_3)}(n-2).\end{aligned}\tag{7.50}$$

2) $v^{-1}_{2j_1+1}\notin N$, 这时 $t(Y)=2(j_1-1)+2^-$. 依据 D 和 $D+D_0$ 的类型的不同取法, 得到 L 中适合条件 (II.2.b) 中情形 2) 的 H 的个数由下面给出

(1) 如果 $t(D)=2^+$, $t(D+D_0)=2^+$, 那么 L 中 H 的个数是

$$\begin{aligned}&\frac{1}{2}qq^{n-2}(q-1)q^{j_1-1}(q^{j_1}-1)\\&\cdot\frac{1}{4}q(q+2)p^{2(j_1-1)+2}_{2(j_2-1)+\delta_2 2(j_3-1)+\delta_3}(n-2).\end{aligned}\tag{7.51}$$

(2) 如果 $t(D)=2^+$, $t(D+D_0)=2^-$, 那么 L 中 H 的个数是

$$\begin{aligned}&\frac{1}{2}qq^{n-2}(q-1)q^{j_1-1}(q^{j_1}-1)\\&\cdot\frac{1}{4}q^2p^{2(j_1-1)+2}_{2(j_2-1)+\delta_2 2(j_3-2+\delta_3)+(2-\delta_3)}(n-2).\end{aligned}\tag{7.52}$$

(3) 如果 $t(D)=2^-$, $t(D+D_0)=2^+$, 那么 L 中 H 的个数是

$$\begin{aligned}&\frac{1}{2}qq^{n-2}(q-1)q^{j_1-1}(q^{j_1}-1)\\&\cdot\frac{1}{4}q^2p^{2(j_1-1)+2}_{2(j_2-2+\delta_2)+(2-\delta_2)2(j_3-1)+\delta_3}(n-2).\end{aligned}\tag{7.53}$$

(4) 如果 $t(D)=2^-$, $t(D+D_0)=2^-$, 那么 L 中 H 的个数是

$$\begin{aligned}&\frac{1}{2}qq^{n-2}(q-1)q^{j_1-1}(q^{j_1}-1)\\&\cdot\frac{1}{4}q(q-2)p^{2(j_1-1)+2}_{2(j_2-2+\delta_2)+(2-\delta_2)2(j_3-2+\delta_3)+(2-\delta_3)}(n-2).\end{aligned}\tag{7.54}$$

综合 (I-ii-3.a), (I-ii-3.b) 两种情形, 由 (7.43)~(7.54) 式, 得到 $|L|$.

综合 (I-i) 和 (I-ii-1), (I-ii-2$'$), (I-ii-3) 中全部情形, 由 (7.16), (7.17), (7.23), (7.42) 和 (7.43)~(7.54) 式, 得到如下的

定理 7.10 对于 $\delta_1=1$, 我们有

$$\begin{aligned}&p^{2j_1+1}_{2j_2+\delta_2 2j_3+\delta_3}(n)\\
=&p^{2j_1+1}_{2j_2+\delta_2 2j_3+\delta_3}(n-1)+f(\delta_2,\delta_3)(q-1)\sum_{l,k}p^{2j_1+1}_{lk}(n-1)\\
&+\frac{1}{2}q^{n-1}(q^{n-1}-q^{2j_1+1})\{(q+1)p^{2j_1+1}_{2(j_2-1)+\delta_2 2(j_3-1)+\delta_3}(n-2)\\
&+(q-1)p^{2j_1+1}_{2(j_2-2+\delta_2)+(2-\delta_2)2(j_3-2+\delta_3)+(2-\delta_3)}(n-2)\}\\
&+\frac{1}{2}q^{n-1}(q^{2j_1}-1)\{(q+1)p^{2(j_1-1)+1}_{2(j_2-1)+\delta_2 2(j_3-1)+\delta_3}(n-2)\\
&+(q-1)\ p^{2(j_1-1)+1}_{2(j_2-2+\delta_2)+(2-\delta_2)2(j_3-2+\delta_3)+(2-\delta_3)}(n-2)\}\\
&+\frac{1}{8}(q-1)q^{n+j_1-1}(q^{j_1}+1)\{(q+2)p^{2j_1}_{2(j_2-1)+\delta_2 2(j_3-1)+\delta_3}(n-2)\\
&+qp^{2j_1}_{2(j_2-1)+\delta_2 2(j_3-2+\delta_3)+(2-\delta_3)}(n-2)+qp^{2j_1}_{2(j_2-2+\delta_2)+(2-\delta_2)2(j_3-1)+\delta_3}(n-2)\\
&+(q-2)p^{2j_1}_{2(j_2-2+\delta_2)+(2-\delta_2)2(j_3-2+\delta_3)+(2-\delta_3)}(n-2)\}\\
&+\frac{1}{8}(q-1)q^{n+j_1-1}(q^{j_1}-1)\{(q+2)\times p^{2(j_1-1)+2}_{2(j_2-1)+\delta_2 2(j_3-1)+\delta_3}(n-2)\\
&+qp^{2(j_1-1)+2}_{2(j_2-1)+\delta_2 2(j_3-2+\delta_3)+(2-\delta_3)}(n-2)+p^{2(j_1-1)+2}_{2(j_2-2+\delta_2)+(2-\delta_2)2(j_3-1)+\delta_3}(n-2)\\
&+(q-2)\times p^{2(j_1-1)+2}_{2(j_2-2+\delta_2)+(2-\delta_2)2(j_3-2+\delta_3)+(2-\delta_3)}(n-2)\}.\end{aligned}$$

到此为止, 我们完成了情形 (I) $2j_1+\delta_1<n$ 的讨论.

(II) $2j_1+\delta_1=n$.

由情形 (I) 的讨论, 以及结合方案参数之间的关系, 只需计算 $p^{2j^+}_{2j^+2j^+}(n)$ 和 $p^{2j+2^-}_{2j+2^-2j+2^-}(n)$. 为此, 先做如下工作.

设

$$U=\begin{pmatrix}Q & V\\ & u\end{pmatrix}.$$

我们来讨论二次型 U 的类型和二次型 Q 的类型之间的关系.

如果 Q 是一个 $n-1$ 阶且型为 $2j+\delta$ 的二次型, 那么存在一个变换 $T \in GL_{n-1}(\mathbb{F}_q)$ 使得

$$U \sim \begin{pmatrix} {}^tT & \\ & 1 \end{pmatrix} U \begin{pmatrix} T & \\ & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & I^{(j)} & & & V_1 \\ & 0 & & & V_2 \\ & & \Delta & & V_3 \\ & & & 0 & V_4 \\ & & & & u \end{pmatrix},$$

这里 ${}^tTV = {}^t({}^tV_1\ {}^tV_2\ {}^tV_3\ {}^tV_4)$. 再令

$$T_1 = \left[I^{(j)}, \begin{pmatrix} I^{(j)} & & V_1 \\ & I^{(n-2j-1)} & \\ & & 1 \end{pmatrix} \right], T_2 = \left[\begin{pmatrix} I^{(j)} & & V_2 \\ & I^{(j)} & \\ & & I^{(n-2j-1)} \end{pmatrix}, 1 \right].$$

那么在"合同"变换 T_1T_2 之下, 得到

$$U \sim \left[\begin{pmatrix} 0 & I^{(j)} \\ & 0 \end{pmatrix}, \begin{pmatrix} \Delta & & V_3 \\ & 0 & V_4 \\ & & u + {}^tV_1V_2 \end{pmatrix} \right].$$

下面来讨论 U 的类型.

(1) $V_4 \neq 0$ 时, 易知 $t(U) = 2(j+1)+\delta$.

(2) $V_4 = 0$ 时, 我们考虑以下三种情形:

(2a) 如果 $\delta = 0$, 那么

$$t(U) = \begin{cases} 2j, & u + {}^tV_1V_2 = 0, \\ 2j+1, & u + {}^tV_1V_2 \neq 0. \end{cases}$$

(2b) 如果 $\delta = 1$, 那么

$$t(U) = \begin{cases} 2j+1, & V_3 = 0, \\ 2(j+1), & V_3 \neq 0,\ V_3^{-2}(u + {}^tV_1V_2) \in N, \\ 2j+2, & V_3 \neq 0,\ V_3^{-2}(u + {}^tV_1V_2) \notin N. \end{cases}$$

(2c) 如果 $\delta = 2$, 那么

$$t(U) = \begin{cases} 2j+2, & u + {}^tV_1V_2 + (a^2+b^2)\alpha + ab = 0, \\ 2(j+1)+1, & u + {}^tV_1V_2 + (a^2+b^2)\alpha + ab \neq 0, \end{cases}$$

这里 $V_3 = {}^t(a, b)$.

由上述讨论可得如下

定理 7.11 对于二次型 U, 我们有

i) 如果 $t(U)=2j$, 那么 Q 的类型可能为 $2(j-1)^+$, $2(j-1)+1$ 或 $2j^+$.

ii) 如果 $t(U)=2j+1$, 那么 Q 的类型可能为 $2(j-1)+1, 2j^+, 2j+1$ 或 $2(j-1)+2^-$.

iii) 如果 $t(U)=2j+2$, 那么 Q 的类型可能为 $2(j-1)+2^-$, $2j+1$ 或 $2j+2^-$.

下面来计算 $p_{2j^+2j^+}^{2j^+}(n)$ 和 $p_{2j+2^-2j+2^-}^{2j+2^-}(n)$.

令 $H_0=0$,

$$H_1=\begin{pmatrix} 0 & I^{(j-1)} & & & X_1 \\ & 0 & & & X_2 \\ & & \Delta & & X_3 \\ & & & 0 & x_{n-1} \\ & & & & x_n \end{pmatrix},$$

这里 ${}^t(X_1X_2X_3)=(x_1,\cdots,x_{n-2})$, $x_i\in\mathbb{F}_q(i=1,\cdots,n-2)$. 令

$$Y=\{(H_1,H)|t(H)=2j+\delta,\ t(H+H_1)=2j+\delta\}.$$

我们区别选取 H_1 和 H 的先后顺序, 对集合 Y 里的元素给出两种计数方法, 可以得到

定理 7.12 设 $n=2j+\delta$, $\delta=0$ 或 2, 那么

$$\begin{aligned} p_{2j+\delta\,2j+\delta}^{2j+\delta}(n)=&\frac{1}{q(q-1)}\{q^{n-2}[p_{2(j-1)+\delta\ 2(j-1)+\delta}^{2(j-1)+\delta}(n-1)\\ &+q(q-1)p_{2(j-1)+\delta\ 2(j-1+\frac{\delta}{2})+1}^{2(j-1)+\delta}(n-1)\\ &+\frac{1}{4}q^2(q-1)^2p_{2(j-1+\frac{\delta}{2})+1\ 2(j-1+\frac{\delta}{2})+1}^{2(j-1)+\delta}(n-1)]\\ &-(q-1)p_{2j+\delta\ 2j+\delta}^{2(j-1+\frac{\delta}{2})+1}(n)-p_{2j+\delta\ 2j+\delta}^{2(j-1)+\delta}(n)\}. \end{aligned}$$

证明 令 $H=\begin{pmatrix} Q & V \\ & u \end{pmatrix}$. 因为 $t(H)=2j+\delta$, 由定理 7.11, 有

(1) 如果 $\delta=0$, 那么 Q 的类型可能为 $2(j-1)$ 或 $2(j-1)+1$.

(2) 如果 $\delta=2$, 那么 Q 的类型可能为 $2(j-1)+2$ 或 $2j+1$.

因此，我们易知,

$$t(H_1)=\begin{cases}2j+\delta, & \text{如果}\, x_{n-1}\neq 0,\, x_i\in\mathbb{F}_q,\\ 2(j-1), & \text{如果}\, x_{n-1}=0,\, x_n+\sum_{i=1}^{j-1}x_ix_{j+i-1}=0,\\ 2(j-1)+2, & \text{如果}\, x_{n-1}=0,\, x_n+\sum_{i=1}^{j-1}x_ix_{j+i-1}\\ & \qquad +(x_{2j-1}^2+x_{2j}^2)\alpha+x_{2j-1}x_{2j}=0,\\ 2(j-1)+1, & \text{如果}\, x_{n-1}=0,\, x_n+\sum_{i=1}^{j-1}x_ix_{j+i-1}\neq 0,\\ 2j+1, & \text{如果}\, x_{n-1}=0,\, x_n+\sum_{i=1}^{j-1}x_ix_{j+i-1}\\ & \qquad +(x_{2j-1}^2+x_{2j}^2)\alpha+x_{2j-1}x_{2j}\neq 0.\end{cases}$$

由此可得

$$\begin{aligned}|Y|=&(q-1)q^{n-1}p_{2j+\delta 2j+\delta}^{2j+\delta}(n)+(q-1)q^{n-2}p_{2j+\delta 2j+\delta}^{2(j-1+\frac{\delta}{2})+1}(n)\\ &+q^{n-2}p_{2j+\delta 2j+\delta}^{2(j-1)+\delta}(n).\end{aligned}\tag{7.55}$$

另一方面, 设

$$W=\left[\begin{pmatrix}0 & I^{(j-1)}\\ & 0\end{pmatrix},\Delta,0^{(n-2(j-1)-\delta-1)}\right],$$

那么

$$H-H_1=\begin{pmatrix}Q-W & V\\ & u\end{pmatrix}.$$

由于 $t(H-H_1)=2j+\delta$, 所以

(1) 如果 $\delta=0$, 那么 $Q-W$ 的类型可能为 $2(j-1)$ 或 $2(j-1)+1$.

(2) 如果 $\delta=2$, 那么 $Q-W$ 的类型可能为 $2(j-1)+2$ 或 $2j+1$.

因为 $t(H)=2j+\delta$, 所以，当 $t(Q)=2(j-1)$, 易知 V,u 有 q^{n-2} 种取法; 当 $t(Q)=2(j-1)+1$, 易知 V,u 有 $\frac{1}{2}q(q-1)q^{n-2}$ 种取法. 取定 V,u 之后, 由于 $t(H-H_1)=2j+\delta$, 我们根据 $Q-W$ 的类型可确定 $x_i(1\leqslant i\leqslant n)$ 的取法个数. 于是得到

$$\begin{aligned}|Y|=&q^{2(n-2)}p_{2(j-1)+\delta\, 2(j-1)+\delta}^{2(j-1)+\delta}(n-1)\\ &+\frac{1}{2}q(q-1)q^{2(n-2)}p_{2(j-1)+\delta\ \ 2(j-1+\frac{\delta}{2})+1}^{2(j-1)+\delta}(n-1)\end{aligned}$$

$$+\frac{1}{2}q(q-1)q^{2(n-2)}p^{2(j-1)+\delta}_{2(j-1+\frac{\delta}{2})+1\ 2(j-1)+\delta}(n-1)$$
$$+\frac{1}{4}q^2(q-1)^2q^{2(n-1)}p^{2(j-1)+\delta}_{2(j-1+\frac{\delta}{2})+1\ 2(j-1+\frac{\delta}{2})+1}(n-1). \tag{7.56}$$

综合 (7.55), (7.56) 两式, 定理得证. □

§7.5 二次型结合方案的对偶性

设 $Q(n, q)$ 表示 $\mathbb{F}_q$ 上 n 元二次型的加法群, $S(n,q)$ 表示 $\mathbb{F}_q$ 上对称矩阵的加法群. 现在给出 $S(n, q)$ 与 $Q(n, q)$ 的特征标群 $Q(n, q)^*$ 的一个同构. 设 χ 是 $\mathbb{F}_q$ 的加法群在复数域 $\mathbb{C}$ 上的一个非平凡不可约特征标. 由于有限交换群的不可约表示都是一次的, 所以有 $\chi : \mathbb{F}_q \to \mathbb{C}^*$, 且 $\chi(x+y) = \chi(x)\chi(y)$, 这里 $x, y \in \mathbb{F}_q$. 因为 $\mathbb{F}_q$ 的特征数为 2, 所以对于任意 $x \in \mathbb{F}_q$, 有 $\chi(x)^2 = 1$. 现在, 对于对称矩阵 $A = (a_{ij}) \in S(n,q)$, 定义

$$\phi_A : [X] \to \phi_A[X] = \chi\left(\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_{ij}\right), \tag{7.57}$$

这里 $X = (x_{ij})$. 我们说这个定义是合理的. 事实上, 如果 $[X] = [Y]$, $Y = (y_{ij})$, 那么 $Y = X + Z$, 而 $Z = (z_{ij})$ 是一个交错矩阵. 于是

$$\begin{aligned}\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}y_{ij} &= \sum_{i=1}^{n} a_{ii}y_{ii} + \sum_{i<j} a_{ij}(y_{ij}+y_{ji}) \\ &= \sum_{i=1}^{n} a_{ii}x_{ii} + \sum_{i<j} a_{ij}(x_{ij}+x_{ji}) \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_{ij},\end{aligned}$$

即 $\phi_A([X]) = \phi_A([Y])$. 显然 ϕ_A 是 $Q(n, q)$ 的一个不可约特征标. 进一步有

定理 7.13 $\phi_A = \phi_B$ 当且仅当 $A = B$. 因而映射 $A \to \phi_A$ 是 $S(n, q)$ 到 $Q(n, q)^*$ 的一个同构. 这样 $S(n, q)$ 可看作 $Q(n, q)$ 的特征标群.

证明 只需证必要性. 设 $\phi_A = \phi_B$(这里 $A = (a_{ij}), B = (b_{ij}) \in S(n,q)$), 即

$$\phi_A([X]) = \phi_B([X]),\ \forall [X] \in Q(n,q),$$

即

$$\chi\left(\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_{ij}\right) = \chi\left(\sum_{i=1}^{n}\sum_{j=1}^{n} b_{ij}x_{ij}\right),\ \forall x_{ij} \in \mathbb{F}_q.$$

对于 i, j 取 $x_{kl} = 0,\ k \neq i, l \neq j$, 那么

$$\chi(a_{ij}x_{ij}) = \chi(b_{ij}x_{ij}),\ \forall x_{ij} \in \mathbb{F}_q.$$

因 $\chi \neq 1$, 所以 $a_{ij} = b_{ij} (i, j = 1, \cdots, n)$, 即 $A = B$.

又 $\phi_{A+B} = \phi_A \phi_B$ 及 $|S(n,q)| = |Q(n,q)^*|$, 立得后一论断. □

定理 7.14 设 $A \in S(n,q)$, $[X] \in Q(n,q)$, 并且 $T \in GL_n(\mathbb{F}_q)$, 那么

$$\phi_{TA\ {}^tT}([X]) = \phi_A([{}^tTXT]).$$

证明 设 $A = (a_{ij})$, $X = (x_{ij})$, $T = (t_{ij})$. 再令 $TA\,{}^tT = (a_{ij}^*)$, 那么 $a_{ij}^* = \sum_{k=1}^n \sum_{l=1}^n t_{ik}a_{kl}t_{jl}$, $a_{ij}^* = a_{ji}^*$. 于是

$$\begin{aligned}\phi_{TA\,{}^tT}([X]) &= \chi\left(\sum_{i=1}^n \sum_{j=1}^n a_{ij}^* x_{ij}\right) = \chi\left(\sum_{i=1}^n \sum_{j=1}^n \sum_{k=1}^n \sum_{l=1}^n t_{ik}a_{kl}t_{jl}x_{ij}\right) \\ &= \chi\left(\sum_{l=1}^n \sum_{k=1}^n a_{kl}\left(\sum_{j=1}^n \sum_{i=1}^n t_{ik}x_{ij}t_{jl}\right)\right) = \phi_A([{}^tTXT]).\end{aligned}$$ □

对于二次型 $[X] \in Q(n,\ q)$, 定义 $S(n,\ q)$ 到 $\mathbb{C}^*$ 的映射

$$\psi_{[X]}(Y) = \phi_Y([X]),\ \forall Y \in S(n,q).$$

那么类似地可以证明 $\psi_{[X]}$ 为 $S(n,q)$ 的不可约特征标, 并且 $[X] \to \psi_{[X]}$ 是 $Q(n,q)$ 到 $S(n,q)^*$($S(n,q)$ 的特征标群) 的一个同构. 因而 $Q(n,q)$ 可看作 $S(n,q)$ 的特征标群. 进一步有

$$\psi_{[TX\ {}^tT]}(Y) = \psi_{[X]}({}^tTYT).$$

定理 7.15 结合方案 $\text{Qua}(n,\ q)$ 和 $\text{Sym}(n,\ q)$ 是形式对偶的.

证明 令 $\text{Qua}(n,\ q)$ 的结合类为 $R_0, R_1, \cdots, R_d$, $d = n + [\frac{n}{2}]$, 并且

$$R_i([0]) = \{[X] \in Q(n,\ q) | ([0],\ [X]) \in R_i\}, i = 0, 1, \cdots, d.$$

那么 $R_i([0])$ 是 $Q(n,\ q)$ 的 "合同" 类. 于是, 任意取定 $[X] \in R_i([0])$, 有

$$R_i([0]) = \{[TX\ {}^tT] | T \in GL_n(\mathbb{F}_q)\},$$

并且 $\mathcal{C} = \{R_i([0]) | i = 0, 1, \cdots, d\}$ 是 $Q(n,\ q)$ 的一个分划. 令 $\mathcal{C}_i$ 表示 "合同" 类 $R_i([0])$ 在 $Q(n,\ q)$ 的群代数 $\mathcal{C}Q(n,\ q)$ 中的形式和. $\mathfrak{S}$ 为由 $\mathcal{C}_0$, $\mathcal{C}_1, \cdots, \mathcal{C}_d$ 生成的 $\mathcal{S}$ 环, 而由 $\mathfrak{S}$ 确定的结合方案 $\mathcal{X}(\mathfrak{S})$ 就是 $\text{Qua}(n,\ q)$. 令

$$\phi_A(\mathcal{C}_i) = \sum_{[X] \in R_i([0])} \phi_A([X]), i = 0, 1, \cdots, d.$$

那么 $\phi_A(\mathcal{C}_i)$ 是 Qua(n, q) 的邻接矩阵 A_i 的特征值, 属于特征向量 ϕ_A. 由定理 7.14, 对于 $A, B \in S(n,\ q)$, 如果 A 合同于 B, 那么

$$\phi_A(\mathcal{C}_i) = \phi_B(\mathcal{C}_i), 0 \leqslant i \leqslant d.$$

由定理 1.14, 在 $Q(n,\ q)^*$ 上确定的等价类恰为

$$Y_j = \{\phi_A | A\text{属于}S(n,\ q)\text{中的合同类}C_j\}.$$

相应地得到 $Q(n,\ q)^*$ 上的 S 环 $\mathfrak{S}^*$. 通过对应 $\phi_A \leftrightarrow A$ 将 $Q(n,\ q)$ 的特征标群 $Q(n,\ q)^*$ 与 $S(n,\ q)$ 等同起来, 由 $\mathfrak{S}^*$ 确定的结合方案就是 Sym$(n,\ q)$. 因此 Qua$(n,\ q)$ 和 Sym$(n,\ q)$ 是形式对偶的. □

一个自然的问题是: 特征数为 2 的二次型结合方案 Qua$(n,\ q)$ 是否自对偶? 我们有

定理 7.16 设 $n \geqslant 2$, 且 $(n, q) \neq (2, 2)$ 或 $(3, 2)$. Qua$(n,\ q)$ 和 Sym$(n,\ q)$ 都不是自对偶的, 因而二者不同构.

证明 令 K_Q 和 K_S 分别表示 Qua$(n,\ q)$ 和 Sym$(n,\ q)$ 的全体价的集合. 设 $q = 2^t$. 由公式 (7.15) 知, K_Q 中 $\gamma = 0$ 时的价 $k_{2s+}(n)$ 所含因数 2 的幂为 $2^{ts^2-1}(1 \leqslant s)$; 而由定理 6.5, K_S 中每个价 $k_{(2\nu+\tau,\tau)}(n)$ 所含因数 2 的幂为 $2^{t\nu(\nu-1)}(\tau = 0, 1 \leqslant \nu)$ 或 $2^{t\nu(\nu+1)}(\tau = 1\text{或}2,\ 0 \leqslant \nu)$. 假如 Qua$(n,\ q)$ 或 Sym$(n,\ q)$ 是自对偶的, 那么由定理 7.15 就有 $K_Q = K_S$. 这样, 对于每个 2^{ts^2-1} 就有 ν 使 $2^{ts^2-1} = 2^{t\nu(\nu-1)}$ 或 $2^{t\nu(\nu+1)}$, 即有 $t(s^2 - \nu(\nu-1)) = 1$ 或 $t(s^2 - \nu(\nu+1)) = 1$. 因而 $t = 1(q = 2), s = 1, \nu = 0$ 或 1, $n \leqslant 3$. 所以当 $(n, q) \neq (2, 2)$ 或 $(3, 2)$ 时, Qua$(n,\ q)$ 和 Sym$(n,\ q)$ 都不是自对偶的, 并且它们不同构. □

定理 7.17 当 $q = 2$ 而 $n = 2$ 或 3 时, 二次型结合方案与对称矩阵结合方案是同构的, 并且都是自对偶的.

证明 (i) 设 $(n, q) = (2, 2)$. 这时 Qua(2, 2) 的价 $k_1 = 3$, $k_{2^+} = 3$, $k_{2^-} = 1$; Sym(2, 2) 的价为 $\overline{k}_1 = 3$, $\overline{k}_2 = 3$, $\overline{k}_{2^*} = 1$. 我们定义映射 $f : Q(2, 2) \to S(2, 2)$,

$$f : A = \begin{pmatrix} a & b \\ & c \end{pmatrix} \longrightarrow \begin{pmatrix} a+b & a+b+c \\ a+b+c & b+c \end{pmatrix}.$$

易见 f 是 $1-1$ 到上的, 并且 $f(0) = 0$, $f(A - B) = f(A) - f(B)$. 进一步,

$$A \in Q_1(2,\ 2) \Leftrightarrow b = 0, a, c\text{不全为}0 \Leftrightarrow \begin{pmatrix} a & a+c \\ a+c & c \end{pmatrix} = f(A) \in S_2(2, 2).$$

$$\begin{aligned} A \in Q_{2^+}(2, 2) &\Leftrightarrow b = 1, a, c\text{ 不全为 }1 \\ &\Leftrightarrow \begin{pmatrix} a+1 & a+c+1 \\ a+c+1 & c+1 \end{pmatrix} = f(A) \in S_1(2, 2). \end{aligned}$$

$$A \in Q_{2^-}(2,2) \Leftrightarrow a = b = c = 1 \Leftrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = f(A) \in S_{2^*}(2,2).$$

所以 Qua(2, 2) 与 Sym(2, 2) 同构.

(ii) 设 $(n, q) = (3, 2)$. 这时, Qua(3,2) 的价 $k_1 = 7$, $k_{2^+} = 21$, $k_{2^-} = 7$, $k_3 = 28$; Sym(2, 2) 的价为 $\overline{k}_1 = 7$, $\overline{k}_2 = 21$, $\overline{k}_{2^*} = 7$, $\overline{k}_3 = 28$. 我们定义映射 $f : Q(3, 2) \to S(3, 2)$,

$$f : A = \begin{pmatrix} d & a & b \\ & e & c \\ & & f \end{pmatrix} \longrightarrow \begin{pmatrix} a & a+b+d & a+c+e \\ a+b+d & b & b+c+f \\ a+c+e & b+c+f & c \end{pmatrix}.$$

显然, $f(0) = 0$, $f(A - B) = f(A) - f(B)$, 并且 f 是 $1-1$ 到上的. 由定理 7.5 可知,

$$A \in Q_1(3, 2) \Leftrightarrow \left\{ \begin{array}{l} a = b = c = 0, \\ d, e, f \text{不全为} 0 \end{array} \right\} \Leftrightarrow \begin{pmatrix} 0 & d & e \\ d & 0 & f \\ e & f & 0 \end{pmatrix} = f(A) \in S_{2^*}(3,2).$$

$$A \in Q_{2^-}(3,2) \Leftrightarrow \left\{ \begin{array}{l} d = a + b + ab, \\ e = a + c + ac, \\ f = b + c + bc, \\ a, b, c \text{不全为} 0 \end{array} \right\} \Leftrightarrow \begin{pmatrix} a & ab & ac \\ ab & b & bc \\ ac & bc & c \end{pmatrix} = f(A) \in S_1(3,2).$$

$$\begin{aligned} A \in Q_3(3,2) &\Leftrightarrow \left\{ \begin{array}{l} a = 1, bc + f + be + cd = 1; \\ \text{或} a = 0, b = 1, e + cd = 1; \\ \text{或} a = b = 0, c = d = 1 \end{array} \right\} \\ &\Leftrightarrow abc + af + be + cd = 1 \\ &\Leftrightarrow \det \begin{pmatrix} a & a+b+d & a+c+e \\ a+b+d & b & b+c+f \\ a+c+e & b+c+f & c \end{pmatrix} = 1 \\ &\Leftrightarrow f(A) \in S_3(3,2). \end{aligned}$$

$$A \in Q_{2^+}(3, 2) \Leftrightarrow f(A) \in S_2(3, 2).$$

所以 Qua(3, 2) 与 Sym(3, 2) 同构. 再由定理 7.15, Qua(3, 2) 和 Sym(3, 2) 都是自对偶的. □

利用本书 §8.8 中关于 Qua(3, q) 的特征值, 可得 Qua(3, 2) 的第一特征值矩阵 P 为

	C_0	C_1	C_{2^*}	C_{2^-}	C_3
f_0	1	7	21	7	28
f_1	1	-1	9	-5	-4
f_2	1	-1	1	3	-4
f_{2^*}	1	7	-3	-1	-4
f_3	1	-1	-3	-1	4

经计算求得 Qua(3, 2) 的第二特征值矩阵 Q 为

$$Q = 64P^{-1} = \begin{pmatrix} 1 & 7 & 21 & 7 & 28 \\ 1 & -1 & -3 & 7 & -4 \\ 1 & 3 & 1 & -1 & -4 \\ 1 & -5 & 9 & -1 & -4 \\ 1 & -1 & -3 & -1 & 4 \end{pmatrix},$$

交换 Q 的 2,4 两行两列则与 P 一致 (注：如果按顺序 $R_0, R_{2^-}, R_{2^+}, R_1, R_3$ 写出 P, 那么求得 Q 将与 P 一致).

§7.6 二次型结合方案的非本原性

从定理 6.1 知, q 为偶数时对称矩阵结合方案 Sym(n, q) 不是本原的. 又从定理 7.15 知, Qua(n, q) 和 Sym(n, q) 是形式对偶的，所以 Qua(n, q) 也不是本原的. 我们先考察 Qua(n, q) 的结合关系图 $\Gamma^{(i)}$ 哪些是连通的, 哪些不是连通的, 进而决定它的结合子方案和相应的商方案.

对于每个 $n \times n$ 交错矩阵 B, 我们令 Q_B 表示以 B 为伴随交错型的那些二次型所成的集合, 即

$$Q_B = \{A \in Q(n, q) | A + {}^tA = B\}.$$

特别是 $Q_0 = \{[a_1, \cdots, a_n] \in Q(n, q) | a_i \in \mathbb{F}_q\}$, 即全体“秩” $\leqslant 1$ 的二次型的集合, 它是 $Q(n, q)$ 的一个加法子群.

定理 7.18 设 q 为偶数且 $(n, q) \neq (3, 2)$. 二次型结合方案 Qua(n, q) 的结合关系图 $\Gamma^{(i)} = (Q(n, q), R_i) (i \neq 0, 1)$ 是连通的；而 $\Gamma^{(1)} = (Q(n, q), R_1)$ 是不连通的, 其连通分支就是那些 $Q_B (B \in K_n)$.

证明 (a) 考虑图 $\Gamma^{(1)} = (Q(n, q), R_1)$, 两个顶点 A 和 C 邻接当且仅当 $(A, C) \in R_1$, 即 $C - A$ 是“秩”为 1 的二次型, 换句话说, $C = A + [d_1, \cdots, d_n]$, 这里 $d_1, \cdots, d_n$ 不全为 0. 由此可知, 顶点 A 和 C 有图 $\Gamma^{(1)}$ 中的道路连接当且仅当 A 和 C 有相同的伴随交错型. 所以 $\Gamma^{(1)}$ 不连通, 并且它的连通分支就是那些 $Q_B (B \in K_n)$. 由 $\Gamma^{(1)}$ 确定的等价关系为 $R_0 \cup R_1$, 每个 Q_B 均为 q^n 个顶点的完全图.

(b) 考虑 $\Gamma^{(2^+)} = (Q(n,q), R_{2^+})$. 往证 $\Gamma^{(2^+)}$ 是连通的. 我们只需证明从任意一个二次型到零二次型都有图 $\Gamma^{(2^+)}$ 中的道路连接, 换句话说, 任意一个非零二次型均可写成类型为 2^+ 的二次型之和. 设 $f = \sum\limits_{i \leqslant j} a_{ij}x_ix_j$. 令 $f_{ij} = a_{ij}x_ix_j$, 这里 $a_{ij} \neq 0$. 如果 $i \neq j$, f_{ij} 是 2^+ 型二次型. 对于项 $f_{ii} = a_{ii}x_i^2 (a_{ii} \neq 0)$, 我们可以写成两个 2^+ 型的二次型之和. 例如, $f_{11} = a_{11}x_1^2 = (a_{11}x_1^2 + x_1x_2) + x_1x_2$, 这里 $a_{11}x_1^2 + x_1x_2$ 和 x_1x_2 均为 2^+ 型的. 这样, f 就可写成 2^+ 型二次型之和. 因而 $\Gamma^{(2^+)}$ 是连通的.

(c) 设 $n \geqslant 3$. 考虑图 $\Gamma^{(i)} (i \neq 1, 2^+, 2^-)$. 往证 $\Gamma^{(i)}$ 是连通的. 只需证明从任意一个二次型 f 到零二次型都有 $\Gamma^{(i)}$ 中的道路连接. 由 (b) 知 $\Gamma^{(2^+)}$ 是连通的, 所以存在 $\Gamma^{(2^+)}$ 中的道路连接 f 和 0. 设此道路为 $0 = f_1, f_2, \cdots, f_m = f$, $(f_i, f_{i+1}) \in R_{2^+}$, 即 $f_i - f_{i+1}$ 的类型为 2^+. 如果我们能够证明交叉数 $p_{ii}^{2^+} \neq 0$, 那么在图 $\Gamma^{(i)}$ 中有道路连接 f_i 和 f_{i+1}, 从而在 $\Gamma^{(i)}$ 中有道路连接 0 和 f. 令 $h = x_1x_n$, 它是 2^+ 型的. 设 $i = 2\nu + \delta$. 我们来选取二次型

$$g = \left[\begin{pmatrix} 0 & I^{(\nu)} \\ & 0 \end{pmatrix}, \ \Delta, \ 0^{(n-2\nu-\delta)} \right],$$

这里 Δ 由 δ 确定. 由于 $i \neq 1, 2^+, 2^-$, 所以 $\nu \geqslant 1$. 易见 g 和 $g+h$ 都是 i 型的, 于是 $p_{ii}^{2^+} \neq 0$. 因此 $\Gamma^{(i)}$ 是连通的.

(d) 剩下的情形为 $i = 2^-$. 考虑图 $\Gamma^{(2^-)}$.

先看 $n = 2$ 的情形. 这时, 由定理 7.4 中的矩阵 B_{2^-} 可知 $p_{2^-2^-}^{2^+}(2) = \frac{1}{4}q(q-1)(q-2)$. 当 $q \neq 2$ 时, $p_{2^-2^-}^{2^+}(2) \neq 0$, 仿 (c) 中的证明可知 $\Gamma^{(2^-)}$ 是连通的.

现在设 $n \geqslant 3$. 当 $q > 2$ 时, 我们可将一个 2×2 的矩阵置于一个 $n \times n$ 矩阵的左上角, 因而就有 $p_{2^-2^-}^{2^+}(n) \neq 0$. 设 $q = 2$. 这时, 我们取 $h = x_1x_3 + x_3^2$, $g = x_1^2 + x_1x_2 + x_2^2$, 那么 h 为 2^+ 型的, 而 g 和 $g+h$ 均为 2^- 型的. 所以也有 $p_{2^-2^-}^{2^+}(n) \neq 0$. 这就证明了图 $\Gamma^{(2^-)}$ 是连通的. □

如果 $(n, q) = (2, 2)$, 那么 Qua(2, 2) 的关系图 $\Gamma^{(2^+)}$ 连通, 且同构于立方体, 而 $\Gamma^{(1)}$ 和 $\Gamma^{(2^-)}$ 均不连通. $\Gamma^{(1)}$ 的连通分支为

$$\left\{ \begin{pmatrix} 0 & 1 \\ & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ & 0 \end{pmatrix}, \begin{pmatrix} 0 & \\ & 1 \end{pmatrix}, \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} \right\}$$

和

$$\left\{ \begin{pmatrix} 0 & \\ & 0 \end{pmatrix}, \begin{pmatrix} 1 & \\ & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \right\},$$

而 $\Gamma^{(2^-)}$ 的连通分支为

$$\left\{ \begin{pmatrix} 0 & \\ & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \right\}, \left\{ \begin{pmatrix} 1 & \\ & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ & 1 \end{pmatrix} \right\}, \left\{ \begin{pmatrix} 0 & \\ & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ & 0 \end{pmatrix} \right\}$$

和

$$\left\{\begin{pmatrix}1 & \\ & 1\end{pmatrix}, \begin{pmatrix}0 & 1\\ & 0\end{pmatrix}\right\}.$$

现在, 我们来阐明 $\mathrm{Qua}(n, q)$ 的结合子方案和相应商方案的结构. 我们有

定理 7.19 特征数为 2 的二次型结合方案 $\mathrm{Qua}(n, q)$ 不是本原的, 它的子方案就是那些 $Q_B(B \in K_n)$, 它们都是平凡的. 相应的商方案同构于交错矩阵结合方案 $\mathrm{Alt}(n, q)$. 对偶地, $\mathrm{Sym}(n, q)$ 不是本原的, 它的子方案就是那些 K_n 在 $S(n, q)$ 中的陪集, 它们均同构于 $\mathrm{Alt}(n, q)$, 而相应的商方案是平凡的.

证明 令 $\overline{Q(n, q)}$ 表示 $Q(n, q)$ 关于子群 Q_0 的商群. $[X]$ 所在的陪集记为 $\overline{[X]}$, 即 $\overline{[X]} = [X] + Q_0$. 显然, $\overline{[X]} = \overline{[Y]}$ 当且仅当 $\overline{[X]} - \overline{[Y]} \in Q_0$, 当且仅当 $\overline{[X]}$ 与 $\overline{[Y]}$ 有相同的交错型. 现在, 建立一个映射

$$\begin{aligned} f : Q(n, q) &\longrightarrow \mathcal{K}(n, q)(n \times n \text{ 交错矩阵的加法群}) \\ [X] &\longmapsto X + {}^tX, \end{aligned}$$

那么 f 是一个到上的群 (加法群) 同态映射, $\mathrm{Ker}\, f = Q_0$. 于是 f 诱导出加法群的同构:

$$\overline{f} : Q(n,q)/Q_0 \to \mathcal{K}(n,q).$$

此外, Q_0 是 $G = GL_n(\mathbb{F}_q) \ltimes Q(n, q)$ 作用下的一个块, 那么 $Q(n, q)$ 关于 Q_0 的全体陪集的集合 $\overline{Q(n, q)}$ 构成 $Q(n, q)$ 的一个非本原系. G 自然地诱导出 $\overline{Q(n, q)}$ 上的作用 $\overline{G}$. 由定理 1.22 知, $(\overline{G}, \overline{Q(n,q)})$ 决定的结合方案同构于商方案 $\mathrm{Qua}(n,q)/Q_0$.

我们来证明$(\overline{G}, \overline{Q(n,q)})$决定的结合方案同构于$n$阶交错矩阵结合方案 $\mathrm{Alt}(n, q)$.

对于 $\overline{(T, [A])} \in \overline{G}$ 及 $\overline{[X]} \in \overline{Q(n,q)}$, 有如下交换图

$$\begin{array}{ccc} \overline{[X]} & \xrightarrow{\overline{f}} & X + {}^tX \\ \overline{(T,[A])}\downarrow & & \downarrow (T, A + {}^tA) \\ \overline{[TX\,{}^tT + A]} & \xrightarrow{\overline{f}} & T(X + {}^tX){}^tT + (A + {}^tA) \end{array}$$

注意到 $\overline{(T, [A])} = \overline{(T,[B])} \Leftrightarrow \overline{[A]} = \overline{[B]} \Leftrightarrow A + {}^tA = B + {}^tB$, 而 $\overline{G}$ 与 $G_1 = GL_n(\mathbb{F}_q) \ltimes \mathcal{K}(n, q)$ 在对应 $\overline{(T, [A])} \mapsto (T, A + {}^tA)$ 之下同构, 所以 $(\overline{G}, \overline{Q(n, q)})$ 与 $(G_1, \mathcal{K}(n, q))$ 等价. 于是 $(\overline{G}, \overline{Q(n, q)})$ 决定的结合方案与 $(G_1, \mathcal{K}(n, q))$ 决定的结合方案同构, 而后者即为 n 阶交错矩阵结合方案 $\mathrm{Alt}(n, q)$. □

§7.7 Qua(n, q) 的两个聚合方案

在这一节中, 我们介绍 $\mathrm{Qua}(n, q)$ 的两个聚合方案, 其中一个是 5.7 中提到的 q 为偶数时的 $\mathrm{Quad}(n, q)$, 另一个是利用二次型的"秩"来确定的结合方案 $\widetilde{\mathrm{Q}}\mathrm{ua}(n, q)$. 由于 $\mathrm{Quad}(n, q)$ 是 $\widetilde{\mathrm{Q}}\mathrm{ua}(n, q)$ 的一个聚合方案, 所以我们先介绍结合方案 $\widetilde{\mathrm{Q}}\mathrm{ua}(n, q)$.

由 7.1 我们知道二次型结合方案 Qua(n, q) 是群 G 可迁地作用在 $Q(n, q)$ 上所确定的结合方案, 这里 G 是 $Q(n, q)$ 的线性自同构群 $GL_n(\mathbb{F}_q)$ 和 $Q(n, q)$ 的平移群所生成的群.Qua(n, q) 的结合类由 $Q(n, q)$ 的“合同”类所确定. 这些“合同”类记作 $Q_i(n, q)$, $i \in J = \{0, 1, 2^+, 2^-, 3, \cdots\}$. 现在, 我们引入 $Q(n, q)$ 的一个自同构群 (但不是线性的), 和 G 一起生成一个群 H. 在 H 作用下我们就可得到 Qua(n, q) 的一个聚合方案 (参看 [12]).

对于 $v \in \mathbb{F}_q^{(n)}$, 我们定义 $Q(n, q)$ 上的变换

$$m_v : [X] \mapsto [X] + [(X + {}^tX)v\, {}^tv(X + {}^tX)].$$

易见 $m_v([X] + [Y]) = m_v([X]) + m_v([Y])$. 又, m_v 是一一的. 实际上, 如果 $m_v([X]) = 0$, 由于 $[(X + {}^tX)v\, {}^tv(X + {}^tX)]$ 的“秩”$\leqslant 1$, 所以 $[X]$ 的“秩”$\leqslant 1$. 于是 $X + {}^tX = 0$. 推出 $[(X + {}^tX)v\, {}^tv(X + {}^tX)] = 0$, 因而 $[X] = 0$. 这样, m_v 是 $Q(n, q)$ 的一个自同构. 进一步, 容易验证 $m_{u+v} = m_u m_v$, 并且由全体 m_v 生成的群 $\langle m_v | v \in \mathbb{F}_q^{(n)} \rangle$ 与 $\mathbb{F}_q^{(n)}$(做为加法群) 同构.

对于 $T \in GL_n(\mathbb{F}_q)$, 由 T 给出 $Q(n, q)$ 的自同构仍用 T 表示, 即 $T : [X] \to [TX\, {}^tT]$. 易见有

$$m_v T = T m_{vT}. \tag{7.58}$$

定理 7.20 关于 $Q(n, q)$ 的自同构群 $\langle m_v | v \in \mathbb{F}_q^{(n)} \rangle$, 我们有

(i) m_v 使每个二次型 $[X]$ 的“秩”不变.

(ii) 对于 $[X] \in Q_{2s^+}(n, q)(Q_{2s^-}(n, q))$, 存在 $v \in \mathbb{F}_q^{(n)}$ 使得 $m_v([X]) \in Q_{2s^-}(n, q)$ $(Q_{2s^+}(n, q))$.

证明 (i) 设 $[X]$ 的“秩”为 $2s$, 那么存在 $T \in GL_n(\mathbb{F}_q)$ 使

$$TX\, {}^tT \equiv M(n, 2s, s) \text{ 或 } M(n, 2(s-1)+2, s-1).$$

不妨设为前一情形 (后一情形同样证明). 注意到

$$M(n, 2s, s) + {}^tM(n, 2s, s) = \left[\begin{pmatrix} 0 & I^{(s)} \\ I^{(s)} & 0 \end{pmatrix}, 0^{(n-2s)} \right],$$

我们有

$$m_v([X]) = \left[T \left(M(n, 2s, s) + \begin{pmatrix} 0 & I^{(s)} & \\ I^{(s)} & 0 & \\ & & 0^{(n-2s)} \end{pmatrix} {}^t(vT) \right.\right.$$

$$\left.\left. (vT) \begin{pmatrix} 0 & I^{(s)} & \\ I^{(s)} & 0 & \\ & & 0^{(n-2s)} \end{pmatrix} \right) {}^tT \right].$$

设 $vT=(v_1,\cdots,v_n)$, 那么

$$m_v([X])=\left[T(M(n,2s,s)+[v_{s+1}^2,\cdots,v_{2s}^2,v_1^2,\cdots,v_s^2,0,\cdots,0])\,{}^tT\right].$$

因而 $m_v([X])$ 的 "秩" 仍为 $2s$.

如果 $[X]$ 的 "秩" 为 $2s+1$, 仿上证明可知 $m_v([X])$ 的 "秩" 仍为 $2s+1$.

(ii) 设 $[X]\in Q_{2s^+}(n,q)$, 不妨设 $X=M(n,2s,s)$. 我们取

$$v=(\underbrace{\alpha^{\frac{1}{2}},0,\cdots,0,}_{s}\alpha^{\frac{1}{2}},0,\cdots,0).$$

易见

$$m_v([X])=\left[\begin{pmatrix}0 & I^{(s)}\\ 0 & 0\end{pmatrix},0^{(n-2s)}\right]+[\underbrace{\alpha,0,\cdots,0,}_{s}\alpha,0,\cdots,0]\in Q_{2s^-}(n,q). \qquad \square$$

另一情形可类似证明之.

现在, 我们令 G_0 是由 $GL_n(\mathbb{F}_q)$ 和 $\langle m_v|v\in\mathbb{F}_q^{(n)}\rangle$ 生成的群, 它也是 $Q(n,q)$ 的一个自同构群. G_0 和 $Q(n,q)$ 的平移群生成作用在 $Q(n,q)$ 上的一个可迁群 H, 因而确定了 $Q(n,q)$ 上的一个结合方案, 记作 $\widetilde{\mathrm{Q}}\mathrm{ua}(n,q)$. 由定理 7.20, G_0 在 $Q(n,q)$ 上的轨道恰为 $Q(n,q)$ 按 "秩" 的分划, 即

$$\widetilde{Q}_i(n,q)=\{[X]\in Q(n,q)|\text{“秩”}=i\},\quad i=0,1,2,\cdots,n.$$

由于 $\widetilde{Q}_{2s+1}(n,q)=Q_{2s+1}(n,q)$, 而 $\widetilde{Q}_{2s}(n,q)=Q_{2s^+}(n,q)\cup Q_{2s^-}(n,q)$, 所以 $\widetilde{\mathrm{Q}}\mathrm{ua}(n,q)$ 为 $\mathrm{Qua}(n,q)$ 的一个聚合方案. 于是, 我们有

定理 7.21 在特征数为 2 的二次型结合方案 $\mathrm{Qua}(n,q)$ 中, 将 "秩" 为 $2s$ 的两个结合关系合并, 记成 $R_{2s}=R_{2s^+}\cup R_{2s^-}$, "秩" 为奇数的结合关系不变. 那么 $\widetilde{\mathrm{Q}}\mathrm{ua}(n,q)=(Q(n,q),\{R_i\}_{0\leqslant i\leqslant n})$ 是一个类数为 n 的对称结合方案.

关于结合方案 $\widetilde{\mathrm{Q}}\mathrm{ua}(n,q)$ 的价, 写 $i=2s+\gamma$, $\gamma=0$ 或 1, 有

$$\widetilde{k}_{2s+\gamma}(n)=\frac{q^{s(s+1)}\displaystyle\prod_{j=s+1}^{n}(q^j-1)}{\displaystyle\prod_{j=1}^{s}(q^j+1)\prod_{j=1}^{n-2s-\gamma}(q^j-1)},\gamma=0\text{ 或 }1. \tag{7.59}$$

由此可知

$$\widetilde{k}_{2s+1}(n)=(q^{n-2s}-1)\widetilde{k}_{2s}(n). \tag{7.60}$$

命题 7.22 结合方案 $\widetilde{\mathrm{Q}}\mathrm{ua}(n,q)$ 的参数 $\widetilde{p}_{1\,j}^{\,k}(n)$ 为

(i) $\widetilde{p}_{1\,j}^{\,2s}(n)=0$, $\widetilde{p}_{1\,j}^{\,2s+1}(n)=0$, $j\notin\{2s,2s+1\}$.

(ii) $\widetilde{p}_{1\,2s}^{\,2s}(n) = q^{2s} - 1$; $\widetilde{p}_{1\,2s+1}^{\,2s}(n) = q^{2s}(q^{n-2s} - 1)$.

(iii) $\widetilde{p}_{1\,2s}^{\,2s+1}(n) = q^{2s}$; $\widetilde{p}_{1,2s+1}^{\,2s+1}(n) = q^n - q^{2s} - 1$.

证明　证明较易, 以 $k = 2s$ 为例说明. 取 $S_1 = 0, S_2 = M(n, 2s, s)$. 设 $S = [v_1, \cdots, v_n]$, 那么

$$S + S_2 = \left[\begin{pmatrix} v_1 & & & & 1 & & \\ & \ddots & & & & \ddots & \\ & & v_s & & & & 1 \\ & & & v_{s+1} & & & \\ & & & & \ddots & & \\ & & & & & & v_{2s} \end{pmatrix}, \begin{pmatrix} v_{2s+1} & & \\ & \ddots & \\ & & v_n \end{pmatrix}\right].$$

“秩” $(S + S_2) = 2s$ 或 $2s + 1$, 所以 (i) 中的第一个等式成立. 如果 $(v_{2s+1}, \cdots, v_n) \neq 0$, 而 $v_1, \cdots, v_{2s}$ 任意, 那么 “秩” $(S + S_2) = 2s + 1$; 如果 $v_{2s+1} = \cdots = v_n = 0$, $v_1, \cdots, v_{2s}$ 不能全为 0, 这时 “秩” $(S + S_2) = 2s$. 所以 (ii) 成立.(iii) 可类似证明. □

接下来, 我们讨论结合方案 $\widetilde{\mathrm{Q}}\mathrm{ua}(n, q)$ 的参数 $\widetilde{p}_{2\,*}^{\,2s}(n)$ 和 $\widetilde{p}_{2\,*}^{\,2s+1}(n)$ 的计算. 由参数关系 $\widetilde{k}_{2s}(n)\widetilde{p}_{2\,*}^{\,2s}(n) = \widetilde{k}_2(n)\widetilde{p}_{2s\,*}^{\,2}(n)$ 和 $\widetilde{k}_{2s+1}(n)\widetilde{p}_{2\,*}^{\,2s+1}(n) = \widetilde{k}_2(n)\widetilde{p}_{2s+1\,*}^{\,2}(n)$ 可知, 要计算 $\widetilde{p}_{2\,*}^{\,2s}(n)$ 和 $\widetilde{p}_{2\,*}^{\,2s+1}(n)$, 只需计算 $\widetilde{p}_{2s\,*}^{\,2}(n)$ 和 $\widetilde{p}_{2s+1\,*}^{\,2}(n)$ 即可.

令 $H_0 = 0$, $H_1 = \left[\begin{pmatrix} 0 & 1 \\ & 0 \end{pmatrix}, 0^{(n-2)}\right]$,

$$M = \{H \in Q(n, q) |\, \text{“秩”}\, (H) = *,\ \text{“秩”}\, (H - H_1) = \diamond\}.$$

那么 $\widetilde{p}_{*\,\diamond}^{\,2}(n) = |M|$. 对于 $H \in M$, 对应于 H_1 做如下分块

$$H = \begin{pmatrix} U & V \\ & W \end{pmatrix},$$

这里 U 为 2 阶方阵, W 为 $n-2$ 阶方阵, V 为 $2 \times (n-2)$ 矩阵. 令

$$M_m = \{H \in M |\, \text{“秩”}\, (W) = m\}.$$

我们有

$$M = \cup_m M_m, \quad |M| = \sum_m |M_m|,$$

这里 $0 \leqslant m \leqslant n - 2$.

任取 $H \in M_m$, 则存在 $g \in G_0$, 使得 $g(0) = 0$, $g(H_1) = H_1$, $g(M_m) = M_m$. 写

$$g(H) \equiv \begin{pmatrix} U & V_1 & V_2 & V_3 & & V_4 \\ & 0 & I^{(\nu)} & & & \\ & & 0 & & & \\ & & & \Delta & & \\ & & & & & 0^{(n-m-2)} \end{pmatrix} \in M_m,$$

这里 $m = 2\nu + \delta$, $\delta = 0$ 或 1. 当 $\delta = 0$ 时, Δ 不出现; 当 $\delta = 1$ 时, $\Delta = (1)$. 我们用 M_m' 表示 M_m 中所有如此形状的 H 的集合. 易见

$$|M_m| = \widetilde{k}_m(n-2)|M_m'|.$$

令

$$A_1 = \left[\begin{pmatrix} I^{(2)} & V_2 \\ & I^{(\nu)} \end{pmatrix}, I^{(\nu)}, I^{(\delta)}, I^{(n-m-2)}\right],$$

$$A_2 = \left[\begin{pmatrix} I^{(2)} & & V_1 \\ & I^{(\nu)} & \\ & & I^{(\nu)} \end{pmatrix}, I^{(\delta)}, I^{(n-m-2)}\right],$$

$$A_2A_1g(H)\ {}^tA_1\ {}^tA_2 \equiv \begin{pmatrix} U_1 & 0 & 0 & V_3 & V_4 \\ & 0 & I^{(\nu)} & & \\ & & 0 & & \\ & & & \Delta & \\ & & & & 0^{(n-m-2)} \end{pmatrix} \in M_m',$$

这里 $U_1 = U + V_1\,{}^tV_2$. 注意到 $A_i0\,{}^tA_i = 0$, $A_iH_1\,{}^tA_i = H_1$, 易见 $A_iM_m'\,{}^tA_i = M_m'$, $i = 1, 2$. 我们将 M_m' 中所有如此形状的 H 作成的集合记作 M_m'', 则

$$|M_m'| = q^{4\nu}|M_m''|.$$

因为 V_4 是 $2\times(n-m-2)$ 矩阵, V_4 的"秩" r 不超过 $\min\{2, (n-m-2)\}$, 所以存在 $P \in GL_{n-m-2}(\mathbb{F}_q)$, 使得 $V_4P = (V_5\ 0)$, 这里 V_5 是一个 $2\times r$ 阵. 令 $A_3 = [I^{(m+2)}, {}^tP]$, 我们有

$$A_3A_2A_1g(H)\ {}^tA_1\ {}^tA_2\ {}^tA_3 \equiv \begin{pmatrix} U_1 & 0 & 0 & V_3 & V_5 & 0 \\ & 0 & I^{(\nu)} & & & \\ & & 0 & & & \\ & & & \Delta & & \\ & & & & 0^{(r)} & \\ & & & & & 0^{(n-m-2-r)} \end{pmatrix} \in M_m''.$$

显然, $A_3 0\, {}^tA_3 = 0, A_3 H_1\, {}^tA_3 = H_1$, 易见 $A_3 M''_m\, {}^tA_3 = M''_m$. 我们将 M''_m 中所有如此形状的 H 作成的集合记作 $M_{(m,r)}$, 则

$$|M''_m| = \sum_r N(r, n-m-2)|M_{(m,r)}|,$$

这里 $N(r, n-m-2)$ 表示 $\mathbb{F}_q^{(n-m-2)}$ 中 r 维子空间的个数, 即

$$N(r, n-m-2) = \frac{\prod\limits_{i=n-m-r-1}^{n-m-2}(q^i-1)}{\prod\limits_{i=1}^{r}(q^i-1)}.$$

综合以上讨论, 我们得到

$$|M_m| = q^{4\nu}\widetilde{k}_m(n-2)\sum_r N(r, n-m-2)|M_{m,r)}|.$$

对于 $H \in M_{(m,r)}$, 它的"秩"由 $\nu(=[\frac{m}{2}])$ 的值和矩阵

$$Q \equiv \begin{pmatrix} U_1 & V_3 & V_5 \\ & \Delta & 0 \\ & & 0 \end{pmatrix}$$

的"秩"所确定. 我们设 $U_1 = \begin{pmatrix} a & b \\ & c \end{pmatrix}$, V_5 是"秩"为 r 的 $2 \times r$ 矩阵. 以下我们分别就 δ 不同的值来讨论 Q 的"秩".

(i) $\delta = 0$.

$$Q \equiv \begin{pmatrix} U_1 & V_5 \\ & 0 \end{pmatrix}.$$

我们区分如下三种情形:

1) $r = 0$ 时,

$$Q \equiv U_1, \text{“秩”}(Q) = \begin{cases} 0, & a = b = c = 0, \\ 1, & b = 0, a, c\text{不全为零}, \\ 2, & b \neq 0. \end{cases}$$

2) $r = 1$ 时, 我们不妨设 $V_5 = {}^t(d_1, d_2)$, 这里 d_1, d_2 不全为零.

$$Q \equiv \begin{pmatrix} a & b & d_1 \\ & c & d_2 \\ & & 0 \end{pmatrix}.$$

由定理 7.5 不难得到,

$$
\text{“秩”}(Q)=\begin{cases}2, & d_1\neq 0, c+bd_1^{-1}d_2+ad_1^{-2}d_2^2=0,\\ & \quad \text{或 } d_1=0,\ d_2\neq 0,\ a=0,\\ 3, & d_1\neq 0, c+bd_1^{-1}d_2+ad_1^{-2}d_2^2\neq 0,\\ & \quad \text{或 } d_1=0,\ d_2\neq 0,\ a\neq 0.\end{cases}
$$

3) $r=2$ 时, 易知 “秩” $(Q)=4$.

(ii) $\delta=1$. 设 $V_3={}^t(v_1,\,v_2)$, 我们考虑如下三种情形:

1) $r=0$ 时,

$$
Q\equiv\begin{pmatrix}a & b & v_1\\ & c & v_2\\ & & 1\end{pmatrix}.
$$

由定理 7.5 知,

$$
\text{“秩”}(Q)=\begin{cases}1, & v_1=v_2=0,\ b=0,\\ 2, & v_1=0, v_2\neq 0,\ a=v_2^{-2}b^2,\\ & \text{或 } v_1\neq 0, c=v_1^{-2}v_2^2a+v_1^{-1}v_2b+v_1^{-2}b^2,\\ 3, & v_1=v_2=0,\ b\neq 0,\\ & \text{或 } v_1=0,\ v_2\neq 0,\ a\neq v_2^{-2}b^2,\\ & \text{或 } v_1\neq 0,\ c\neq v_1^{-2}v_2^2a+v_1^{-1}v_2b+v_1^{-2}b^2.\end{cases}
$$

2) $r=1$. 类似于情形 i), 我们不妨设 $V_5={}^t(d_1,\,d_2)$.

若 $d_1\neq 0$,

$$
Q\equiv\begin{pmatrix}a & b & v_1 & d_1\\ & c & v_2 & d_2\\ & & 1 & 0\\ & & & 0\end{pmatrix}\sim\begin{pmatrix}a & b & v_1 & d_1\\ & c^* & v_2+v_1d_1^{-1}d_2 & 0\\ & & 1 & 0\\ & & & 0\end{pmatrix}
$$

$$
\sim\begin{pmatrix}0 & 0 & 0 & d_1\\ & c^* & v_2+v_1d_1^{-1}d_2 & 0\\ & & 1 & 0\\ & & & 0\end{pmatrix},
$$

这里 $c^*=c+bd_1^{-1}d_2+ad_1^{-2}d_2^2$.

若 $d_1 = 0$, $d_2 \neq 0$,

$$Q \equiv \begin{pmatrix} a & b & v_1 & 0 \\ & c & v_2 & d_2 \\ & & 1 & 0 \\ & & & 0 \end{pmatrix} \sim \begin{pmatrix} a & 0 & v_1 & 0 \\ & 0 & 0 & d_2 \\ & & 1 & 0 \\ & & & 0 \end{pmatrix}.$$

由此可知

$$\text{“秩”}(Q) = \begin{cases} 3, & d_1 \neq 0,\ v_2 + v_1 d_1^{-1} d_2 = 0, \\ & \text{或 } d_1 = 0,\ d_2 \neq 0,\ v_1 = 0, \\ 4, & d_1 \neq 0,\ v_2 + v_1 d_1^{-1} d_2 \neq 0, \\ & \text{或 } d_1 = 0, d_2 \neq 0, v_1 \neq 0. \end{cases}$$

3) $r = 2$ 时, 不难得到 “秩” $(Q) = 5$.

上面的分析给出了计算 $\widetilde{p}_{*\diamond}^{2}$ 的一种方法. 注意到, 我们在对 H 所作的“合同”变换中, H_1 始终不变. 因此我们适当选取 ν 的值和 Q 的“秩”, 使得 “秩” $(H) = *$. 同时, 以 $b+1$ 替换 b, 得到相应的 Q_1, 选取适当的 Q_1, 使之与 ν 的值满足 “秩” $(H - H_1) = \diamond$. 根据 ν 及 Q 和 Q_1 的 “秩” 所要求的相应条件, 计算出 $|M_{(m,r)}|$, 乘以相应的因子, 再求和, 就可计算出 $\widetilde{p}_{*\diamond}^{2}$. 特别地, 我们可以用此方法计算出 $\widetilde{p}_{2s\ *}^{2}(n)$ 和 $\widetilde{p}_{2s+1\ *}^{2}(n)$, 再利用参数关系计算出 $\widetilde{p}_{2\ *}^{2s}(n)$ 和 $\widetilde{p}_{2\ *}^{2s+1}(n)$. 于是我们有

命题 7.23　结合方案 $\widetilde{\mathrm{Q}}\mathrm{ua}(n, q)$ 的参数 $\widetilde{p}_{2\ j}^{k}(n)$ 为

(i) $\widetilde{p}_{2j}^{2s}(n) = 0$, $j \notin \{2S-2,\ 2s-1,\ 2s,\ 2s+1,\ 2s+2\}$;

$\widetilde{p}_{2j}^{2s+1}(n) = 0$, $j \notin \{2s-1,\ 2s,\ 2s+1,\ 2s+2,\ 2s+3,\}$.

(ii) $\widetilde{p}_{2\,2s-2}^{2s}(n) = \frac{q^{2s-2}(q^{2s}-1)}{q^2-1}$;

$\widetilde{p}_{2\,2s-1}^{2s}(n) = q^{2s-2}(q^{2s}-1)$;

$\widetilde{p}_{2\,2s}^{2s}(n) = \frac{(q^{2s}-1)(q^{n+1}+q^n-2q^{2s}-q^2)}{q^2-1}$;

$\widetilde{p}_{2\,2s+1}^{2s}(n) = q^{2s}(q^{2s}-1)(q^{n-2s}-1)$;

$\widetilde{p}_{2\,2s+2}^{2s}(n) = \frac{q^{4s+2}(q^{n-2s}-1)(q^{n-2s-1}-1)}{q^2-1}$.

(iii) $\widetilde{p}_{2\,2s-1}^{2s+1}(n) = \frac{q^{2s}(q^{2s}-1)}{q^2-1}$;

$\widetilde{p}_{2\,2s}^{2s+1}(n) = q^{2s}(q^{2s}-1)$;

$\widetilde{p}_{2\,2s+1}^{2s+1}(n) = \frac{(q^{2s}-1)(q^{n+2}+q^{n+1}-2q^{2s+2}-q^2)}{q^2-1}$;

$\widetilde{p}_{2\,2s+2}^{2s+1}(n) = q^{4s+2}(q^{n-2s-1}-1)$;

$$\widetilde{p}^{2s+1}_{2\,2s+3}(n) = \frac{q^{4s+4}(q^{n-2s-1}-1)(q^{n-2s-2}-1)}{q^2-1}.$$

注：命题 7.23(ii) 和 (iii) 的参数计算过程中，利用参数之间关系，只需直接计算四个参数 $\widetilde{p}^{2s}_{2\,2s+1}(n)$, $\widetilde{p}^{2s}_{2\,2s+2}(n)$, $\widetilde{p}^{2s+1}_{2\,2s+2}(n)$ 和 $\widetilde{p}^{2s+1}_{2\,2s+3}(n)$ 即可，这里不再赘述.

下面我们叙述二次型结合方案 Qua(n, q) 的另一聚合方案 Quad(n, q). 令 $\overline{R}_0 = R_0$, $\overline{R}_i = R_{2i-1} \cup R^+_{2i} \cup R^-_{2i-1} = R_{2i-1} \cup R_{2i}$, $1 \leqslant i \leqslant [\frac{n+1}{2}]$. 我们有

命题 7.24 对于 $i, j \in \{0, 1, \cdots, [\frac{n+1}{2}]\}$,

$$p_{i,1,j} = |\{Q \in Q(n, q) | (Q_1, Q) \in \overline{R}_1, (Q, Q_2) \in \overline{R}_i\}|$$

是常数，只要 $(Q_1, Q_2) \in \overline{R}_j$, 这里

(i) $p_{i,1,j} = 0$, 如果 $|i-j| > 1$,

(ii) $p_{i-1,1,i} = \frac{q^{2i-2}(q^{2i}-1)}{q^2-1}$,

(iii) $p_{i,1,i} = \frac{(q^{2i}-1)(q^{n+1}+q^n-q^{2i}-q^{2i-2}-1)}{q^2-1}$,

(iv) $p_{i+1,1,i} = \frac{q^{4i}(q^{n-2i}-1)(q^{n-2i+1}-1)}{q^2-1}$.

证明 设 $t = 2j-1$ 或 $2j$. 任意取定 $(Q_1, Q_2) \in \overline{R}_t$, 那么有

$$p_{i,1,j} = \widetilde{p}^t_{1\,2i-1} + \widetilde{p}^t_{1\,2i} + \widetilde{p}^t_{2\,2i-1} + \widetilde{p}^t_{2\,2i}.$$

由命题 7.22 和命题 7.23 直接验证可知 (i)~(iv) 成立. □

令 Γ 为 $\overline{R}_1$ 的图. 容易看出，$\overline{R}_i$ 恰为 Γ 中距离为 i 的顶点对子的集合. 由命题 7.24 可知 Γ 为距离正则的. 于是我们得到

定理 7.25([4]) 设 $n \geqslant 2$. $(Q(n, q), \{\overline{R}_i\}_{0 \leqslant i \leqslant [\frac{n+1}{2}]})$ 是一个 P 多项式结合方案，记作 Quad(n, q).

通常文献中称图 $\Gamma = (Q(n, q), \overline{R}_1)$ 为 $\mathbb{F}_q$ 上二次型图，记为 Quad(n, q). 这个图与交错矩阵的图 Alt$(n+1, q)$ 有相同的参数. [4] 中通过对此图 Γ 中两邻接顶点的奇异线进行了分析，特别对于 $q = 2$ 的情形采用非常技巧性的处理，证明了下面的

定理 7.26 设 $n \geqslant 3$ 且 $(n, q) \neq (3, 2)$. 那么图 $\Gamma = (Q(n, q), \overline{R}_1)$ 不是距离可迁的. 因而结合方案 Quad(n, q) 与 Alt$(n+1), q)$ 不同构.

对于 $(n, q) = (3, 2)$, 由定理 7.17 知 Qua$(3, 2)$ 同构于 Sym$(3, 2)$, 并且在给出的同构对应下使得 Quad$(3, 2)$ 同构于 $\overline{\text{Sym}}(3, 2)$. 再由定理 6.13 知 $\overline{\text{Sym}}(3, 2)$ 同构于 Alt$(4, 2)$. 于是 Quad$(3, 2)$ 与 Alt$(4, 2)$ 同构.

§7.8 二次型结合方案的自同构

在这一节中，我们讨论二次型结合方案 Qua(n, q) 的自同构. 首先，容易证明

定理 7.27 设 $n \geqslant 2$, q 为 2 的方幂. 我们有

$$\text{Aut}\quad \text{Qua}(n, q) = \text{Inn}\quad \text{Qua}(n, q).$$

证明　考察结合关系 $R_{2s+\gamma}$ 的价 $k_{2s+\gamma}(n)(2s+\gamma \neq 0)$ 中的偶数因子. 设 $q = 2^t, t \geqslant 1$. 当 $\gamma = 0, 1, 2$ 时, 由 (7.15) 式可以得到 $k_{2s+\gamma}(n)$ 中的偶数因子分别为 2^{ts^2-1}, $2^{ts(s+1)}$, $2^{t(s+1)^2-1}$. 由此可知, 当 $t \geqslant 2$ 即 $q \geqslant 4$ 时, 如果 $k_{2s_1+\gamma_1}(n) = k_{2s_2+\gamma_2}(n)$, 那么一定有 $\gamma_1 = 0$, $\gamma_2 = 2$, $s_1 = s_2 + 1$. 但此时

$$k_{2s_1+\gamma_1}(n)/k_{2s_2+\gamma_2}(n) = (q^{s_1}+1)/(q^{s_1}-1) \neq 1.$$

于是 k_i, $i = 1, 2^+, 2^-, 3, \cdots$ 两两不等. 由推论 1.28 可得结论.

当 $q = 2$ 时, 如果 $k_{2s_1+\gamma_1}(n) = k_{2s_2+\gamma_2}(n)$, 那么可能有以下两种情形:

(i) $\gamma_1 = 0$, $s_1 = 1$, $\gamma_2 = 1$, $s_2 = 0$;

(ii) $\gamma_1 = 1$, $\gamma_2 = 2$, $s_1 = s_2 = 0$.

由 (i) 可得 $q^{n-1} - 1 = q - 1$. 因而 $n = 2$, $k_1(2) = k_{2^+}(2) = 3$. 但由定理 7.4 可知 Qua(2, 2) 的参数 $p_{11}^1(2) = 2$, $p_{2^+2^+}^{2^+}(2) = 0$. 再由定理 1.27 可得结论. 由 (ii) 可得 $q^{n-1} - 1 = q + 1$, 因而 $n = 3$, $k_1(3) = k_{2^-}(3) = 7$. 此时, 由定理 7.6 可知 $p_{11}^1(3) = 6$, $p_{2^-2^-}^{2^-}(3) = 0$. 再由定理 1.27 可得结论. □

由此定理可知, $\text{Qua}(n, q)$ 的自同构群恰为全体 $\Gamma^{(i)} = (Q(n, q), R_i)(i \neq 0)$ 的自同构群之交. 明显地, $Q(n, q)$ 上一个形如

$$X \mapsto {}^tPX^\sigma P + Y, \ \forall X \in Q(n, q) \tag{7.61}$$

的变换是结合方案 $\text{Qua}(n, q)$ 的一个自同构, 这里 $P \in GL_n(\mathbb{F}_q)$, σ 是 $\mathbb{F}_q$ 的一个自同构, $Y \in Q(n, q)$. 我们要证明 $\text{Qua}(n, q)$ 的每个自同构具有这种形状.

令 G_n 表示 $\text{Qua}(n,q)$ 的全体形如 (7.61) 的自同构作成的群. 我们有

$$G_n \subseteq \text{Aut}\quad \text{Qua}(n,q) \subseteq \cap_{i\in\{1,2^+,2^-\}}\text{Aut}\Gamma^{(i)} \subseteq \text{Aut}\quad \text{Quad}(n, q).$$

[12] 中证明了下面的

定理 7.28　设 q 为 2 的方幂, $n \geqslant 3$ 并且 $(n, q) \neq (3, 2)$. 那么 $\text{Quad}(n, q)$ 的全自同构群为 G_n 和群 $\langle m_v | v \in \mathbb{F}_q^{(n)}\rangle$ 的乘积.

现在, 我们来证明本节的主要定理

定理 7.29　设 $n \geqslant 2$, q 为 2 的方幂. 那么, 二次型结合方案 $\text{Qua}(n, q)$ 的全自同构群就是 G_n.

证明　区分下面几种情形.

(i) $n \geqslant 3$ 且 $(n, q) \neq (3, 2)$.

由定理 7.28 知, 这时 $\text{Quad}(n, q)$ 的全自同构群由群 G_n 和群 $\langle m_v | v \in \mathbb{F}_q^{(n)}\rangle$ 生成. $\text{Quad}(n, q)$ 的关系图 $\Gamma = (Q(n, q), \overline{R}_1)$ 的边集为 $\text{Qua}(n, q)$ 的三个关系图

$\Gamma^{(1)}$, $\Gamma^{(2^+)}$ 和 $\Gamma^{(2^-)}$ 的边集之并, 即 $\overline{R}_1 = R_1 \cup R_{2^+} \cup R_{2^-}$. 由定理 7.27 知, 结合方案 Qua$(n, q)$ 的自同构 $\mathcal{A}$ 自然地也是 Γ 的自同构, 因而 $\mathcal{A}$ 可表为 G_n 的元素与某个 m_v 之积. 进一步由定理 7.20 知, 如果 m_v 非单位元, 那么 $m_v \notin \mathrm{Aut}\Gamma^{(2^+)}$, 于是 $\mathcal{A} \in G_n$. 这样, Aut Qua$(n, q) = G_n$.

(ii) $(n, q) = (3, 2)$.

此时, 由定理 7.17 可知 Qua(3,2) 同构于 Sym(3,2), 于是 $|\mathrm{Aut\ Qua}(3, 2)| = |\mathrm{Aut\ Sym}(3,2)|$. 进一步由定理 6.14, $|\mathrm{Aut\ Sym}(3,2)|=|G_3|$. 又因 $G_3 \subseteq \mathrm{Aut\ Qua}(3, 2)$, 所以 Aut Qua$(3, 2) = G_3$.

(iii) $(n, q) = (2, 2)$.

这时, 由定理 7.17, Qua(2,2) 同构于 Sym(2,2). 进一步由定理 6.14, $|\mathrm{Aut\ Sym}(2, 2)| = |G_2|$. 所以可得 Aut Qua$(2, 2) = G_2$.

(iv) $n = 2$ 且 $q \geqslant 4$.

我们来证明: 这时 $\mathrm{Aut}\Gamma^{(2^+)} = G_2$, 从而得 Aut Qua$(2, q) = G_2$. 证明分以下九步. 设 $\mathcal{A} \in \Gamma^{(2^+)}$, 那么 $\mathcal{A}(X) - \mathcal{A}(Y) \in Q_{2^+}(2, q)$ 当且仅当 $X - Y \in Q_{2^+}(2, q)$.

第一步. $\mathcal{A}$ 将零二次型 0 映到 $\mathcal{A}(0)$. 用 G_2 中的自同构 $X \mapsto X - \mathcal{A}(0)$ 乘以 $\mathcal{A}$ 之后, 不妨设 $\mathcal{A}(0) = 0$. 再用 G_2 中的自同构 $X \mapsto {}^tPXP$, $P \in GL_2(\mathbb{F}_q)$ 乘以 $\mathcal{A}$ 之后, 我们可以进一步假设 $\mathcal{A}\begin{pmatrix} 0 & 1 \\ & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ & 0 \end{pmatrix}$.

第二步. 设 $U = \left\{ \begin{pmatrix} 0 & x \\ & 0 \end{pmatrix} \middle| x \in \mathbb{F}_q \right\}$, 我们断言 $\mathcal{A}(U) = U$. 否则, 假设存在 $\begin{pmatrix} 0 & a \\ & 0 \end{pmatrix} \in U, a \neq 0, 1$, 使得 $\mathcal{A}\begin{pmatrix} 0 & a \\ & 0 \end{pmatrix} = \begin{pmatrix} m & b \\ & n \end{pmatrix}$, 而 m, n 不全为 0. 我们将导出矛盾. 不失一般性, 我们可以假设 $m \neq 0$. 用 G_2 中的自同构 $X \mapsto {}^tP_1XP_1$, $P_1 = \left[m^{-\frac{1}{2}}, m^{\frac{1}{2}}\right]$ 乘以 $\mathcal{A}$ 之后, 进一步可设 $m = 1$. G_2 中的这个自同构使 0 和 $\begin{pmatrix} 0 & 1 \\ & 0 \end{pmatrix}$ 都不动. 而且 $\begin{pmatrix} 0 & a \\ & 0 \end{pmatrix} \in Q_{2^+}(2, q)$, $\begin{pmatrix} 0 & a \\ & 0 \end{pmatrix} - \begin{pmatrix} 0 & 1 \\ & 0 \end{pmatrix} \in Q_{2^+}(2, q)$. 于是我们有 $\begin{pmatrix} 1 & b \\ & n \end{pmatrix} \in Q_{2^+}(2, q)$, $\begin{pmatrix} 1 & b \\ & n \end{pmatrix} - \begin{pmatrix} 0 & 1 \\ & 0 \end{pmatrix} \in Q_{2^+}(2, q)$. 因此 $b \neq 0, 1$, $n \in b^2N \cap (b+1)^2N$.

现在令

$$S_1 = \left\{ X \in Q_{2^+}(2, q) \middle| X - \begin{pmatrix} 0 & 1 \\ & 0 \end{pmatrix} \in Q_{2^+}(2, q), X - \begin{pmatrix} 0 & a \\ & 0 \end{pmatrix} \in Q_{2^+}(2, q) \right\},$$

$$S_2 = \left\{ X \in Q_{2^+}(2, q) \middle| X - \begin{pmatrix} 0 & 1 \\ & 0 \end{pmatrix} \in Q_{2^+}(2, q), X - \begin{pmatrix} 1 & b \\ & n \end{pmatrix} \in Q_{2^+}(2, q) \right\}.$$

因 $\mathcal{A}$ 使 0 不动, $\mathcal{A}(Q_{2^+}(2, q)) = Q_{2^+}(2, q)$. 又因 $\mathcal{A}\begin{pmatrix}0 & 1\\ & 0\end{pmatrix} = \begin{pmatrix}0 & 1\\ & 0\end{pmatrix}$, $\mathcal{A}\begin{pmatrix}0 & a\\ & 0\end{pmatrix} = \begin{pmatrix}1 & b\\ & n\end{pmatrix}$, 我们有 $\mathcal{A}(S_1) = S_2$, $|S_1| = |S_2|$. 然而, 通过下面的计算我们将得到 $|S_1| \neq |S_2|$, 导致矛盾.

首先计算 $|S_1|$, 这里

$$S_1 = \left\{ \begin{pmatrix} y & x \\ & z \end{pmatrix} \middle| x^{-2}yz \in N, (x+1)^{-2}yz \in N, (x+a)^{-2}yz \in N \right\}.$$

显然 $x \neq 0, 1, a$.

(1) 当 $y = 0$ 时, x 有 $q-3$ 种取法. 取定 x 之后, z 有 q 种取法. 在此情形下, 适合 S_1 中条件的二次型个数为 $q^2 - 3q$.

(2) 设 $y \neq 0$, y 有 $q-1$ 种取法. 取定 y 之后, z 有 $|x^2N \cap (x+1)^2N \cap (x+a)^2N|$ 种取法. 注意到 x^{-2}, $(x+1)^{-2}$ 和 $(x+a)^{-2}$ 两两不等, 并且 $x^{-2} + (x+1)^{-2} + (x+a)^{-2} = 0$ 当且仅当 $x = a^{\frac{1}{2}}$.

当 $x \neq a^{\frac{1}{2}}$, x 有 $q-4$ 种取法. 取定 x 之后, 由定理 7.3 可知 z 有 $q/8$ 种取法.

当 $x = a^{\frac{1}{2}}$, 注意到 $aN \cap (a+1)N \subset (a+a^2)N$, 由定理 7.3, z 有 $|aN \cap (a+1)N| = q/4$ 种取法.

因此, 当 $y \neq 0$ 时, 适合 S_1 中条件的二次型个数为 $q^3/8 - 3q^2/8 + q/4$.

综合 (1) 和 (2) 得

$$|S_1| = q^3/8 + 5q^2/8 - 11q/4. \tag{7.62}$$

接下来计算 $|S_2|$, 这里

$$S_2 = \left\{ \begin{pmatrix} y & x \\ & z \end{pmatrix} \middle| x^{-2}yz \in N, (x+1)^{-2}yz \in N, (x+b)^{-2}(y+1)(z+n) \in N \right\}.$$

显然, $x \neq 0, 1, b$.

(1) 当 $y = 0$ 时, x 有 $q-3$ 种取法. 取定 x 之后, z 有 $|(x+b)^2N + n| = q/2$ 种取法. 此时, 适合 S_2 中条件的二次型个数为 $q^2/2 - 3q/2$.

(2) 当 $y = 1$ 时, x 有 $q-3$ 种取法. 取定 x 之后, z 有 $|x^2N \cap (x+1)^2N| = q/4$ 种取法. 此时, 适合 S_2 中条件的二次型个数为 $q^2/4 - 3q/4$.

(3) 设 $y \neq 0, 1$. 我们先来考察 $x^{-2}y$, $(x+1)^{-2}y$ 和 $(x+b)^{-2}(y+1)$ 在 $\mathbb{F}_2$ 上的线性关系. 在所设条件下, $x^{-2}y$, $(x+1)^{-2}y$ 和 $(x+b)^{-2}(y+1)$ 均不等于 0, 且 $x^{-2}y + (x+1)^{-2}y \neq 0$. 又不难导出

$$x^{-2}y + (x+b)^{-2}(y+1) = 0 \Leftrightarrow y = b^{-2}x^2.$$

$$(x+1)^{-2}y + (x+b)^{-2}(y+1) = 0 \Leftrightarrow y = (b+1)^{-2}(x+1)^2.$$

$$x^{-2}y + (x+1)^{-2}y + (x+b)^{-2}(y+1) = 0 \Leftrightarrow y(x^2+b)^2 = (x^2+x)^2.$$

我们区分 $x=b^{\frac{1}{2}}$ 和 $x\neq b^{\frac{1}{2}}$ 两种情形.

(a) $x=b^{\frac{1}{2}}$.

当 $y=b^{-1}$ 时, $x^2y^{-1}=b^2$, $(x+1)^2y^{-1}=b^2+b$, $(x+b)^2(y+1)^{-1}=b^2$, 所以 $z\in b^2N\cap(b^2+b)N\cap(b^2N+n)$. 由于 $n\in b^2N$, z 有 $q/4$ 种取法.

当 $y=(b+1)^{-1}$ 时, $z\in(b^2+b)N\cap(b+1)^2N\cap[(b+1)^2N+n]$. 由于 $n\in(b+1)^2N$, z 有 $q/4$ 种取法.

当 $y\neq 0,1,b^{-1},(b+1)^{-1}$ 时, y 有 $q-4$ 种取法. 此时 $x^{-2}y,(x+1)^{-2}y,(x+b)^{-2}(y+1)$ 在 $\mathbb{F}_2$ 上线性无关, 由定理 7.3 知 z 有 $q/8$ 种取法.

因此, 当 $x=b^{\frac{1}{2}}$ 时, 适合 S_2 中条件的二次型个数为 $q^2/8$.

(b) $x\neq b^{\frac{1}{2}}$. 因为 $x\neq 0,1,b,b^{\frac{1}{2}}$, x 有 $q-4$ 种取法.

当 $y=b^{-2}x^2$ 时, $z\in b^2N\cap b^2(1+x^{-2})N\cap(b^2N+n)$. 因为 $n\in b^2N$, z 有 $q/4$ 种取法.

当 $y=(b+1)^{-2}(x+1)^2$ 时, $z\in(b+1)^2[1+(x+1)^{-2}]N\cap(b+1)^2N\cap[(b+1)^2N+n]$. 因为 $n\in(b+1)^2N$, z 有 $q/4$ 种取法.

当 $y=(x^2+b)^{-2}(x^2+x)^2$ 时, $z\in(x+1)^{-2}(x^2+b)^2N\cap x^{-2}(x^2+b)^2N\cap[(x^2+b)^2N+n]$. 因为 $(x+1)^{-2}N\cap x^{-2}N\subset N$, 所以, 如果 $(x^2+b)^{-2}n\in N$, 那么 z 有 $q/4$ 种取法; 如果 $(x^2+b)^{-2}n\notin N$, 那么 z 的取法数为 0. 因此, z 的取法数 $\leqslant q/4$.

当 $y\neq 0$, 1, $b^{-2}x^2$, $(b+1)^{-2}(x+1)^2$, $(x^2+b)^{-2}(x^2+x)^2$ 时, y 有 $q-5$ 种取法. 此时, $x^{-2}y$, $(x+1)^{-2}y$, $(x+b)^{-2}(y+1)$ 在 $\mathbb{F}_2$ 上线性无关. 由定理 7.3 知, z 有 $q/8$ 种取法.

因此, 当 $x\neq b^{\frac{1}{2}}$ 时, 适合 S_2 中条件的二次型个数 $\leqslant q^3/8-3q^2/8-q/2$.

由 (1)~(3) 可得

$$|S_2|\leqslant q^3/8+q^2/2-11q/4. \tag{7.63}$$

从 (7.62) 和 (7.63) 两式得 $|S_2|<|S_1|$, 导致矛盾. 于是我们有 $\mathcal{A}(U)=U$.

第三步. 由 $\mathcal{A}(U)=U$ 可知, $\mathcal{A}$ 在 $\mathbb{F}_q$ 上诱导了一个一一映射, 记作 σ_1, 使得对于任意 $\begin{pmatrix}0 & a\\ & 0\end{pmatrix}\in U$, $\mathcal{A}\begin{pmatrix}0 & a\\ & 0\end{pmatrix}=\begin{pmatrix}0 & \sigma_1(a)\\ & 0\end{pmatrix}$, 且 $\sigma_1(0)=0$, $\sigma_1(1)=1$. 往证对于任意二次型 $\begin{pmatrix}y & a\\ & z\end{pmatrix}$, 均有 $\mathcal{A}\begin{pmatrix}y & a\\ & z\end{pmatrix}=\begin{pmatrix}y' & \sigma_1(a)\\ & z'\end{pmatrix}$.

设 Y 是图 $\Gamma^{(2^+)}$ 的任意一点, 令 $Y^{\perp}=\{X|X-Y\in Q_{2^+}(2,q)\}$ 表示图 $\Gamma^{(2^+)}$ 中所有与 Y 邻接的二次型的集合. $S^{\perp}=\cap_{Y\in S}Y^{\perp}$ 表示所有与点集 S 中每个二次型都邻接的二次型的集合. 相应地, $Y^*=\{X|X-Y\notin Q_{2^+}(2,q)\}$, $S^*=\cap_{Y\in S}Y^*$.

对于 $a\in\mathbb{F}_q$, 令 $W_a=\left[U\Big\backslash\begin{pmatrix}0 & a\\ & 0\end{pmatrix}\right]^{\perp}$. 易见 $W_a=\left\{\begin{pmatrix}y & a\\ & z\end{pmatrix}\middle| yz=0\right\}$. 实际

上, 设 $X=\begin{pmatrix} y & x \\ & z \end{pmatrix} \in W_a$, 那么 $\begin{pmatrix} y & x \\ & z \end{pmatrix}-\begin{pmatrix} 0 & b \\ & 0 \end{pmatrix} \in Q_{2+}(2,q), \forall b \in \mathbb{F}_q, b \neq a$. 于是 $x=a$ 且对于任意 $b \in \mathbb{F}_q, b \neq a$, 均有 $(a-b)^{-2}yz \in N$. 由此可得 $yz=0$. 进一步, 我们有 $W_a^* = \left\{\begin{pmatrix} y & a \\ & z \end{pmatrix} \middle| y,z \in \mathbb{F}_q\right\}$. 因为 $\mathcal{A}\begin{pmatrix} 0 & a \\ & 0 \end{pmatrix} = \begin{pmatrix} 0 & \sigma_1(a) \\ & 0 \end{pmatrix}$, $\mathcal{A}(U)=U$, 所以 $\mathcal{A}(W_a)=W_{\sigma_1(a)}$ 且 $\mathcal{A}(W_a^*)=W_{\sigma_1(a)}^*$.

第四步. $W_0 = \left\{\begin{pmatrix} y & \\ & z \end{pmatrix} \middle| yz=0\right\}$. 由 $\sigma_1(0)=0$ 得 $\mathcal{A}(W_0)=W_0$. 因此 $\mathcal{A}\begin{pmatrix} 1 & \\ & 0 \end{pmatrix} = \begin{pmatrix} m & \\ & 0 \end{pmatrix}$ 或 $\mathcal{A}\begin{pmatrix} 1 & \\ & 0 \end{pmatrix} = \begin{pmatrix} 0 & \\ & m \end{pmatrix}$, $m \neq 0$. 类似于第二步的讨论, 我们可以假设 $\mathcal{A}\begin{pmatrix} 1 & \\ & 0 \end{pmatrix} = \begin{pmatrix} 1 & \\ & 0 \end{pmatrix}$.

第五步. 令 $W_a^+ = \left\{\begin{pmatrix} y & a \\ & 0 \end{pmatrix} \middle| y \in \mathbb{F}_q\right\}$, $W_a^- = \left\{\begin{pmatrix} 0 & a \\ & z \end{pmatrix} \middle| z \in \mathbb{F}_q\right\}$, 那么 $W_a = W_a^+ \cup W_a^-$. 往证 $\mathcal{A}(W_0^+)=W_0^+$, $\mathcal{A}(W_0^-)=W_0^-$, $\mathcal{A}(W_a^+)=W_{\sigma_1(a)}^+$, $\mathcal{A}(W_a^-)=W_{\sigma_1(a)}^-$.

由 $\sigma_1(1)=1$ 得 $\mathcal{A}(W_1)=W_1$. 令 $S=\begin{pmatrix} 1 & \\ & 0 \end{pmatrix}^* \cap W_1$. 经计算可知 $S=\left\{\begin{pmatrix} 0 & 1 \\ & m \end{pmatrix} \middle| m \notin N\right\}$. 因 $\mathcal{A}\begin{pmatrix} 1 & \\ & 0 \end{pmatrix} = \begin{pmatrix} 1 & \\ & 0 \end{pmatrix}$, $\mathcal{A}(W_1)=W_1$, 于是有 $\mathcal{A}(S)=S$.

断言 $S^\perp \cap W_0 = W_0^-$. 实际上, 设 $\begin{pmatrix} y & x \\ & z \end{pmatrix} \in S^\perp \cap W_0$, 可得 $x=0, yz=0$ 且 $y(z+m) \in N$, $\forall m \notin N$, 即 $ym \in N$, $\forall m \notin N$. 立得 $y=0$. 于是有 $S^\perp \cap W_0 = W_0^-$. 由 $\mathcal{A}(S)=S$, $\mathcal{A}(W_0)=W_0$ 可得 $\mathcal{A}(W_0^-)=W_0^-$, 进而有 $\mathcal{A}(W_0^+)=W_0^+$.

现在, 易见 $W_a^+ = (W_0^+)^\perp \cap W_a$, $W_a^- = (W_0^-)^\perp \cap W_a$. 于是 $\mathcal{A}(W_a^+)=W_{\sigma_1(a)}^+$, $\mathcal{A}(W_a^-)=W_{\sigma_1(a)}^-$.

第六步. 由于 $\mathcal{A}(W_0^+)=W_0^+$, $\mathcal{A}$ 在 $\mathbb{F}_q$ 上诱导出一个一一映射 σ_2, 使得对于任意 $[a,0] \in W_0^+$, 有 $\mathcal{A}[a,0]=[\sigma_2(a),0]$, 并且 $\sigma_2(0)=0$, $\sigma_2(1)=1$. 往证对于任意 $\begin{pmatrix} a & x \\ & z \end{pmatrix} \in Q(2,q)$, 均有 $\mathcal{A}\begin{pmatrix} a & x \\ & z \end{pmatrix} = \begin{pmatrix} \sigma_2(a) & \sigma_1(x) \\ & z' \end{pmatrix}$.

令 $L_1=[a,0]^\perp \cap W_1^-$. 经计算可知 $L_1=\left\{\begin{pmatrix} 0 & 1 \\ & a^{-1}n \end{pmatrix} \middle| n \in N\right\}$. 由 $\mathcal{A}[a,0]=[\sigma_2(a),0]$, $\mathcal{A}(W_1^-)=W_1^-$, 可得

$$\mathcal{A}(L_1)=\left\{\begin{pmatrix} 0 & 1 \\ & [\sigma_2(a)]^{-1}n \end{pmatrix} \middle| n \in N\right\}.$$

其次, 令 $L_2=[L_1^\perp \cap (W_0^* \setminus W_0)] \cup [a,0]$, 那么 $L_2=\{[a, a^{-1}n] \| n \in N\}$.

实际上, 设 $\begin{pmatrix} y & x \\ & z \end{pmatrix} \in L_2$, $\begin{pmatrix} y & x \\ & z \end{pmatrix} \neq \begin{pmatrix} a & \\ & 0 \end{pmatrix}$, 由 $\begin{pmatrix} y & x \\ & z \end{pmatrix} \in W_0^* \setminus W_0$ 可得 $x = 0$, $yz \neq 0$. 再由 $[y,\ z] \in L_1^\perp$ 得 $y(z + a^{-1}n) \in N$, $\forall n \in N$, 即 $a^{-1}yN + yz = N$. 应用定理 7.3 得 $y = a$, $z \in a^{-1}N$. 现在, 由 $\mathcal{A}(W_0^*) = W^*_{\sigma_1(0)} = W_0^*$, $\mathcal{A}(W_0) = W_0$, $\mathcal{A}\begin{pmatrix} a & \\ & 0 \end{pmatrix} = \begin{pmatrix} \sigma_2(a) & \\ & 0 \end{pmatrix}$, 我们得到

$$\mathcal{A}(L_2) = \left\{ \begin{pmatrix} \sigma_2(a) & \\ & [\sigma_2(a)]^{-1}n \end{pmatrix} \middle| n \in N \right\}.$$

再次, 令 $L_3 = L_2^\perp \cap (W_1^* \setminus W_1^-)$, 经计算可得 $L_3 = \left\{ \begin{pmatrix} a & 1 \\ & z \end{pmatrix} \middle| z \in \mathbb{F}_q \right\}$. 由 $\mathcal{A}(W_1^*) = W^*_{\sigma_1(1)} = W_1^*$, $\mathcal{A}(W_1^-) = W_1^-$, 可得 $\mathcal{A}(L_3) = \left\{ \begin{pmatrix} \sigma_2(a) & 1 \\ & z \end{pmatrix} \middle| z \in \mathbb{F}_q \right\}$.

最后, $L_3^\perp = \left\{ \begin{pmatrix} a & x \\ & z \end{pmatrix} \middle| x, z \in \mathbb{F}_q, x \neq 1 \right\}$. $\mathcal{A}(L_3^\perp) = [\mathcal{A}(L_3)]^\perp$, 即

$$\mathcal{A}(\left\{ \begin{pmatrix} a & x \\ & z \end{pmatrix} \middle| x, z \in \mathbb{F}_q, x \neq 1 \right\}) = \left\{ \begin{pmatrix} \sigma_2(a) & x \\ & z \end{pmatrix} \middle| x, z \in \mathbb{F}_q, x \neq 1 \right\}.$$

进一步, 因为 $\mathcal{A}(L_3) = \left\{ \begin{pmatrix} \sigma_2(a) & 1 \\ & z \end{pmatrix} \middle| z \in \mathbb{F}_q \right\}$, 所以对于任意 $\begin{pmatrix} a & x \\ & z \end{pmatrix} \in Q(2,\ q)$, 均有 $\mathcal{A}\begin{pmatrix} a & x \\ & z \end{pmatrix} = \begin{pmatrix} \sigma_2(a) & \sigma_1(x) \\ & z \end{pmatrix}$.

类似地, 由于 $\mathcal{A}(W_0^-) = W_0^-$, 可以证明 $\mathcal{A}$ 在 $\mathbb{F}_q$ 上诱导出一个一一映射 σ_3, 使得对于任意 $\begin{pmatrix} y & x \\ & z \end{pmatrix} \in Q(2,q)$, 均有 $\mathcal{A}\begin{pmatrix} y & x \\ & z \end{pmatrix} = \begin{pmatrix} \sigma_2(y) & \sigma_1(x) \\ & \sigma_3(z) \end{pmatrix}$, 并且 $\sigma_3(0) = 0$.

第七步. 以下我们证明 $\sigma_2 = \sigma_3$. 首先考察 σ_3 与 σ_1 之间的关系.

由 $\mathcal{A}(W_0^-) = W_0^-$ 可设 $\mathcal{A}[0,\ 1] = [0,\ m]$, 这里 $m = \sigma_3(1)$. 令 $H_1 = [0, 1]^\perp \cap W_1^+ = \left\{ \begin{pmatrix} n & 1 \\ & 0 \end{pmatrix} \middle| n \in N \right\}$. 由 $\mathcal{A}(W_1^+) = W_1^+$ 可得

$$\mathcal{A}(H_1) = [0,\ m]^\perp \cap W_1^+ = \left\{ \begin{pmatrix} m^{-1}n & 1 \\ & 0 \end{pmatrix} \middle| n \in N \right\}.$$

令 $H_2 = H_1^\perp \cap (W_0^* \setminus W_0) = \{[n,\ 1] | n \in N,\ n \neq 0\}$. 由 $\mathcal{A}(W_0^* \setminus W_0) = W_0^* \setminus W_0$, $\mathcal{A}(H_2) = [\mathcal{A}(H_1)]^\perp \cap (W_0^* \setminus W_0)$, 可得 $\mathcal{A}(H_2) = \{[m^{-1}n, m] | n \in N, n \neq 0\}$.

令 $H_3 = (H_2 \cup \{[0,\ 1]\})^\perp$. 若 $\begin{pmatrix} y & x \\ & z \end{pmatrix} \in H_3$, 那么 $x \neq 0$, $x^{-2}(y+n)(z+1) \in N$, $\forall n \in N$. 显然, 对于任意 $x, y \in \mathbb{F}_q$, $x \neq 0$, $\begin{pmatrix} y & x \\ & 1 \end{pmatrix} \in H_3$. 当 $z \neq 1$ 时, 由

$x^{-2}(z+1)N + x^{-2}(z+1)y = N$ 可知 $x^{-2}(z+1) = 1, y \in N$, 即 $z = x^2+1, y \in N$. 因此,

$$H_3 = \left\{ \begin{pmatrix} y & x \\ & x^2+1 \end{pmatrix} \middle| x \in \mathbb{F}_q^*, \, y \in N \right\} \cup \left\{ \begin{pmatrix} y & x \\ & 1 \end{pmatrix} \middle| x, \, y \in \mathbb{F}_q, \, x \neq 0 \right\}.$$

由于 $\mathcal{A}[0,\ 1] = [0,\ m]$, 我们有 $\mathcal{A}(H_3) = [\mathcal{A}(H_2) \cup \{[0,\ m]\}]^{\perp}$. 仿 H_3 的计算可得

$$\mathcal{A}(H_3) = \left\{ \begin{pmatrix} m^{-1}y & x \\ & m(x^2+1) \end{pmatrix} \middle| x \in \mathbb{F}_q^*, y \in N \right\} \cup \left\{ \begin{pmatrix} y & x \\ & m \end{pmatrix} \middle| x, y \in \mathbb{F}_q, x \neq 0 \right\}.$$

因为 $\sigma_3(1) = m$, 由第六步, 我们有

$$\mathcal{A}\left(\left\{ \begin{pmatrix} y & x \\ & 1 \end{pmatrix} \middle| x, \, y \in \mathbb{F}_q, x \neq 0 \right\} \right) = \left\{ \begin{pmatrix} y & x \\ & m \end{pmatrix} \middle| x, y \in \mathbb{F}_q, x \neq 0 \right\},$$

立得

$$\mathcal{A}\left(\left\{ \begin{pmatrix} y & x \\ & x^2+1 \end{pmatrix} \middle| x \in \mathbb{F}_q^*, y \in N \right\} \right) = \left\{ \begin{pmatrix} m^{-1}y & x \\ & m(x^2+1) \end{pmatrix} \middle| x \in \mathbb{F}_q^*, y \in N \right\},$$

即 $\sigma_3(1)[(\sigma_1(x))^2+1] = \sigma_3(x^2+1)$.

与上述讨论类似, 以 $[1,\ 0]$ 替代 $[0,\ 1]$. 以 W_1^- 替代 W_1^+, 我们就得到 σ_2 与 σ_1 之间的关系 $\sigma_2(1)[(\sigma_1(x))^2+1] = \sigma_2(x^2+1)$. 因 $\sigma_2(1) = 1$, 于是 $(\sigma_1(x))^2+1 = \sigma_2(x^2+1)$. 代入前面 σ_1 与 σ_3 的关系式, 得到 $\sigma_3(1)\sigma_2(x^2+1) = \sigma_3(x^2+1)$, $\forall x \in \mathbb{F}_q^*$. 此式对 $x = 0$ 也成立, 于是可得

$$\sigma_3(1)\sigma_2(x) = \sigma_3(x), \ \forall x \in \mathbb{F}_q.$$

余下只需证明 $\sigma_3(1) = 1$ 即可得 $\sigma_2 = \sigma_3$.

令 $M = [1,\ 0]^{\perp} \cap W_1^- = \left\{ \begin{pmatrix} 0 & 1 \\ & n \end{pmatrix} \middle| n \in N \right\}$. 由 $\mathcal{A}[1,\ 0] = [1,\ 0]$, $\mathcal{A}(W_1^-) = W_1^-$, 得 $\mathcal{A}(M) = M$. 又由于 $\mathcal{A}(M) = \left\{ \begin{pmatrix} 0 & 1 \\ & \sigma_3(n) \end{pmatrix} \middle| n \in N \right\}$, 立得 $\sigma_3(N) = N$. 现在考察集合

$$I = \left\{ \begin{pmatrix} x & 1 \\ & x \end{pmatrix} \middle| x \in N \right\}, \mathcal{A}(I) = \left\{ \begin{pmatrix} \sigma_2(x) & 1 \\ & \sigma_3(x) \end{pmatrix} \middle| x \in N \right\}.$$

对于 $x \in N$, 恒有 $x^2 \in N$. 因此 $I \subset Q_{2^+}(2,q)$. 又由 $\mathcal{A}(Q_{2^+}(2,q)) = Q_{2^+}(2,q)$ 得 $\mathcal{A}(I) \subset Q_{2^+}(2,q)$, 即得 $\sigma_2(x)\sigma_3(x) \in N, \forall x \in N$. 由 $\sigma_3(1)\sigma_2(x) = \sigma_3(x)$ 立得 $[\sigma_3(1)]^{-1}(\sigma_3(x))^2 \in N$, $\forall x \in N$. 再由 $\sigma_3(N) = N$ 可得 $[\sigma_3(1)]^{-1}N = N$. 于是 $\sigma_3(1) = 1$, 进而有 $\sigma_2 = \sigma_3$.

第八步. 往证 σ_2 是 $\mathbb{F}_q$ 的一个自同构.

(i) 我们先证明 σ_2 是 $\mathbb{F}_q$ 的一个加法同态. 更一般地, 我们证明 $a_1, \cdots, a_m$ 在 $\mathbb{F}_2$ 上线性无关当且仅当 $\sigma_2(a_1), \cdots, \sigma_2(a_m)$ 在 $\mathbb{F}_2$ 上也线性无关.

由于 $[a_i,\ 0] \in W_0^+$, 我们有 $\mathcal{A}[a_i,\ 0] = [\sigma_2(a_i),\ 0], i = 1, 2, \cdots, m$. 设 $D = \left\{ \begin{pmatrix} 0 & 1 \\ & z \end{pmatrix} \middle| z \in \mathbb{F}_q \right\}$. 由 $\sigma_1(1) = 1$ 和 $\sigma_2(0) = 0$ 知, $\mathcal{A}(D) = D$. 考察集合

$$S_1 = \{X \in D | X - [a_i,\ 0] \in Q_{2^+}(2,\ q),\ i = 1, \cdots, m\}$$

和

$$S_2 = \{X \in D | X - [\sigma_2(a_i)\ 0] \in Q_{2^+}(2,\ q),\ i = 1, \cdots, m\}.$$

我们有 $\mathcal{A}(S_1) = S_2$, $|S_1| = |S_2|$. 由于

$$|S_1| = \left| \left\{ \begin{pmatrix} 0 & 1 \\ & z \end{pmatrix} \middle| z \in a_i^{-1}N,\ i = 1, \cdots, m \right\} \right|,$$

$$|S_2| = \left| \left\{ \begin{pmatrix} 0 & 1 \\ & z \end{pmatrix} \middle| z \in [\sigma_2(a_i)]^{-1}N,\ i = 1, \cdots, m \right\} \right|.$$

应用定理 7.3 立得结论. 因此, 进一步有 $\sigma_2(a + b) = \sigma_2(a) + \sigma_2(b)$.

(ii) 再证 $\sigma_2(x^{-1}) = (\sigma_2(x))^{-1}$, $\forall x \in \mathbb{F}_q^*$.

由 $\sigma_2(1) = 1$ 和 $\sigma_3(1) = 1$ 知 $\mathcal{A}[1,\ 1] = [1,\ 1]$. 考察集合 $K_1 = [1,\ 1]^{\perp} \cap U = \left\{ \begin{pmatrix} 0 & a \\ & 0 \end{pmatrix} \middle| a \neq 0,\ a^{-2} \in N \right\}$. 令 $K_2 = K_1^{\perp} \cap (W_0^* \setminus W_0)$. 简单计算可得 $K_2 = \{[x,\ x^{-1}] | x \in \mathbb{F}_q^*\}$. 因 $\mathcal{A}(U) = U$, $\mathcal{A}(W_0^* \setminus W_0) = W_0^* \setminus W_0$, 我们有 $\mathcal{A}(K_2) = K_2$. 再利用 $\sigma_2 = \sigma_3$ 得 $\sigma_2(x^{-1}) = (\sigma_2(x))^{-1}$, $\quad \forall x \in \mathbb{F}_q^*$.

综合 (i) 和 (ii), 以及 $\sigma_2(1) = 1$, 由华罗庚关于体的自同构定理可知 σ_2 是 $\mathbb{F}_q$ 的一个自同构.

第九步. 最后, 我们证明 $\sigma_1 = \sigma_2 (= \sigma_3)$.

由第七步的讨论知 $[\sigma_1(x)]^2 + 1 = \sigma_2(x^2 + 1)$. 因 σ_2 是 $\mathbb{F}_q$ 的一个自同构. 于是 $\sigma_2(x^2 + 1) = [\sigma_2(x)]^2 + 1$. 因此, $\sigma_1(x) = \sigma_2(x)$, $\forall x \in \mathbb{F}_q$, 即 $\sigma_1 = \sigma_2$.

我们将 $\sigma_1, \sigma_2, \sigma_3$ 统一记为 σ. 于是对于任意 $X \in Q(2,\ q)$, $\mathcal{A}(X) = X^{\sigma}$. 至此, 我们完成了情形 $n = 2$ 的证明. □

注: 对于 $n \geqslant 3$, 也可采用矩阵方法直接确定关系图 $\Gamma^{(2^+)}$ 的自同构群, 从而给出结合方案 Qua$(n,\ q)$ 的自同构群 (参看 [23]).

第八章　二次型结合方案的特征值

§8.1　Qua(2, q) 的特征值

本章中恒设 q 为 2 的方幂. 我们主要讨论 $\mathbb{F}_q$ 上 n 元二次型结合方案 Qua(n,q) 的特征值, 给出它们的某些递推计算公式和性质, 进而导出 Qua(n,q) 的聚合方案 $\widetilde{\text{Q}}$ua(n,q) 和 Quad(n,q) 在 $\mathbb{F}_q$ 上 $n\times n$ 对称矩阵结合方案 Sym (n,q) 中形式对偶方案.

为了书写方便, 将 $\mathbb{F}_q$ 上型为 k 的 n 元二次型的 "合同类" 记为 $C_k^{(n)}$, $k\in\{0,1,2^+,2^-,3,\cdots\}$. 又将 $\mathbb{F}_q$ 上秩为 r 的 n 阶非交错矩阵的合同类记为 $D_r^{(n)}, r=0,1,\cdots,n$; 而将秩为 $2s$ 的 n 阶交错矩阵的合同类记为 $D_{2s^*}^{(n)}$, $s=1,2,\cdots,\ [\frac{n}{2}]$.

设 χ 是 $\mathbb{F}_q$ 的加法群在复数域 $\mathbb{C}$ 的一个非平凡不可约特征标, 对于每个对称矩阵 $A\in S(n,q)$, $A=(a_{ij})$, 如下定义加法群 $Q(n,q)$ 的特征标

$$f_A:[X]\longmapsto f_A([X])=\chi\left(\sum_{i,j=1}^{n}a_{ij}x_{ij}\right),\tag{8.1}$$

这里 $X=(x_{ij})$ 为 $\mathbb{F}_q$ 上的 $n\times n$ 矩阵. 由定理 7.14 知

$$f_{TA^tT}([X])=f_A([^tTXT]).$$

令

$$f_A(C_j^{(n)})=\sum_{[X]\in C_j^{(n)}}f_A([X]),\ \ j=0,\,1,\,2^+,\,2^-,\,3,\,\cdots.$$

由定理 7.15 知, 对称矩阵 A 和 B 属于 $S(n,q)$ 的一个合同类 $D_i^{(n)}$ $(i=0,1,2,2^*,3,\cdots)$. 当且仅当

$$f_A(C_j^{(n)})=f_B(C_j^{(n)}),\ j=0,\,1,\,2^+,\,2^-,\,3.\,\cdots.$$

我们用 $f_i^{(n)}$ 表示 $S(n,q)$ 的合同类 $D_i^{(n)}$ 中的矩阵依 (8.1) 给出的特征标, 那么 Qua(n,q) 的第一特征值矩阵 P 的 (i,j) 元素就是 $f_i^{(n)}(C_j^{(n)})$.

下面我们计算 $\mathbb{F}_q$ 上 2 元二次型结合方案 Qua$(2,q)$ 的特征值. 为此, 我们取上三角矩阵作为二次型的代表元. $Q(2,q)$ 有四个 "合同" 类, 它们有如下的代表元:

$$A_0=0,\,A_1=\begin{pmatrix}1&0\\&0\end{pmatrix},\,A_{2^+}=\begin{pmatrix}0&1\\&0\end{pmatrix},\,A_{2^-}=\begin{pmatrix}\alpha&1\\&\alpha\end{pmatrix}$$

(这里 α 是 $\mathbb{F}_q$ 中取定的一个不属于 N 的元). 它们所代表的二次型的类型分别是 0, 1, 2^+ 和 2^-, 那么

$$C_0 = \{0\},\ C_1 = \left\{ \begin{pmatrix} x & 0 \\ & z \end{pmatrix} \middle|\ x,\ z\text{不全为 } 0 \right\},$$

$$C_{2^+} = \left\{ \begin{pmatrix} x & y \\ & z \end{pmatrix} \middle|\ y \neq 0,\ y^{-2}xz \in N \right\},$$

$$C_{2^-} = \left\{ \begin{pmatrix} x & y \\ & z \end{pmatrix} \middle|\ y \neq 0,\ y^{-2}xz \notin N \right\}.$$

我们在定理 7.4 中已算出 Qua(2, q) 的价为 $k_0 = |C_0| = 1$, $k_1 = |C_1| = q^2 - 1$, $k_{2^+} = |C_{2^+}| = \frac{1}{2}q(q^2-1)$, $k_{2^-} = |C_{2^-}| = \frac{1}{2}q(q-1)^2$.

另一方面, 对于 $\mathbb{F}_q$ 上 2×2 对称矩阵的合同类, 取如下代表元:

$$S_0 = 0,\ S_1 = \begin{pmatrix} 1 & \\ & 0 \end{pmatrix},\ S_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ S_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

那么,

$$\phi_0 = \phi_{\begin{pmatrix} 0 & \\ & 0 \end{pmatrix}} = 1,\ \phi_1 = \phi_{\begin{pmatrix} 1 & \\ & 0 \end{pmatrix}},\ \phi_2 = \phi_{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}},\ \phi_3 = \phi_{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}$$

是 $Q(2, q)$ 的特征标群 $Q(2, q)^*$ 的等价类的代表元. 将 "合同" 类 C_0, C_1, C_{2^+} 和 C_{2^-} 依次改记为 C_0, C_1, C_2 和 C_3. 那么由定理 1.16, Qua(2, q) 的第一特征值矩阵 P 的 (i, j) 元素为

$$\phi_i(C_j) = \sum_{X \in C_j} \phi_i(X),\ i, j = 0, 1, 2, 3.$$

下面具体算出 $\phi_i(C_j)$ 之值. 计算过程中要用到 $|N| = q/2$ 和关于特征标 χ 的如下等式:

$$\sum_{x \in \mathbb{F}_q} \chi(x) = 0.$$

显然

$$\phi_j(C_0) = 1,\ j = 0, 1, 2, 3.$$

$$\phi_0(C_i) = k_i,\ i = 0, 1, 2, 3.$$

$$\phi_1(C_1)=\sum_{X\in C_1}\phi_{\begin{pmatrix}1&\\&0\end{pmatrix}}(X)=\sum_{x,z\text{ 不全为 }0}\chi(x)$$
$$=\sum_{z\neq 0}\chi(0)+q\sum_{x\neq 0}\chi(x)=q-1-q=-1.$$
$$\phi_1(C_2)=\sum_{X\in C_2}\phi_{\begin{pmatrix}1&\\&0\end{pmatrix}}(X)$$
$$=\sum_{y\neq 0,\,xz\in y^2N}\chi(x)=\sum_{y\neq 0,\,x=0,\,z\text{ 任意}}\chi(0)+\sum_{y\neq 0,\,x\neq 0,\,z\in x^{-1}y^2N}\chi(x)$$
$$=q(q-1)+\frac{1}{2}q(q-1)\sum_{x\neq 0}\chi(x)=q(q-1)-\frac{1}{2}q(q-1)=\frac{1}{2}q(q-1).$$
$$\phi_1(C_3)=\sum_{X\in C_3}\phi_{\begin{pmatrix}1&\\&0\end{pmatrix}}(X)=\sum_{y\neq 0,\,xz\notin y^2N}\chi(x)$$
$$=\sum_{x\neq 0}\chi(x)\left[(q-1)\cdot\frac{q}{2}\right]=-\frac{1}{2}q(q-1).$$
$$\phi_2(C_1)=\sum_{X\in C_1}\phi_{\begin{pmatrix}1&\\&1\end{pmatrix}}(X)$$
$$=\sum_{x,z\text{ 不全为 }0}\chi(x)\chi(z)=\sum_{x\text{ 任意}}\chi(x)\sum_{z\text{ 任意}}\chi(z)-\chi(0)\chi(0)=-1.$$

类似地算出 Qua(2, q) 的第一特征值矩阵

$$P=\begin{pmatrix}1 & q^2-1 & \frac{1}{2}q(q^2-1) & \frac{1}{2}q(q-1)^2\\ 1 & -1 & \frac{1}{2}q(q-1) & -\frac{1}{2}q(q-1)\\ 1 & -1 & -\frac{1}{2}q & \frac{1}{2}q\\ 1 & q^2-1 & -\frac{1}{2}q(q+1) & -\frac{1}{2}q(q-1)\end{pmatrix}.$$

求出 Qua(2, q) 的第二特征值矩阵

$$Q=q^3P^{-1}=\begin{pmatrix}1 & q^2-1 & (q-1)(q^2-1) & q-1\\ 1 & q-1 & -(q-1) & -1\\ 1 & -1 & -(q-1) & q-1\\ 1 & -(q+1) & q+1 & -1\end{pmatrix}.$$

如果交换 Q 的第 2, 3 行, 这相当于将 Qua(2, q) 的结合关系按 R_0, R_{2+}, R_1, R_{2-} 排序, 那么 Qua(2, q) 的第二特征值矩阵与定理 6.2 中算出的二阶对称矩阵结合方案 Sym(2, q) 的第一特征值矩阵

$$\begin{pmatrix} 1 & q^2-1 & (q-1)(q^2-1) & q-1 \\ 1 & q-1 & -(q-1) & -1 \\ 1 & -1 & -(q-1) & q-1 \\ 1 & -(q+1) & q+1 & -1 \end{pmatrix}$$

完全一致.

§8.2 关于 χ 的几条引理

设 $\mathbb{F}_q$ 为 q 元有限域, $\operatorname{char}\mathbb{F}_q = 2$. 又设 χ 是 $\mathbb{F}_q$ 的加法群 $(\mathbb{F}_q, +)$ 在复数域 $\mathbb{C}$ 上的一个非平凡不可约特征标, x, v_1, v_2, $\cdots$ 是在 $\mathbb{F}_q$ 中取值的变量.

引理 8.1

$$\sum_{\substack{v_1, \cdots, v_m \text{满足某个条件} \\ \text{但 } x \text{任意}}} \chi(x) = 0.$$

证明 设满足条件的元素组 $(v_1, \cdots, v_m)$ 的个数为 s, 那么立知

$$\sum_{\substack{v_1, \cdots, v_m \text{满足某个条件} \\ \text{但} x \text{任意}}} \chi(x) = s \cdot \sum_{x \in \mathbb{F}_q} = \chi(x) = s \cdot 0 = 0.$$ □

引理 8.2

$$\sum_{(v_1, \cdots, v_{2i}) \in \mathbb{F}_q^{(2i)}} \chi\left(\sum_{j=1}^{i} v_j v_{i+j}\right) = q^i.$$

证明 先证明它对于 $i = 1$ 时成立. 实际上, 这时我们有

$$\begin{aligned} \sum_{(v_1, v_2) \in \mathbb{F}_q^{(2)}} \chi(v_1 v_2) &= \sum_{v_1 = 0 \text{ 或 } v_2 = 0} \chi(0) + \sum_{v_1 \neq 0} \sum_{v_2 \neq 0} \chi(v_1 v_2) \\ &= 2q - 1 + (q-1)(-1) = q. \end{aligned}$$

对 i 施行归纳法, 有

$$\begin{aligned} &\sum_{(v_1, \cdots, v_{2i}) \in \mathbb{F}_q^{(2i)}} \chi\left(\sum_{j=1}^{i} v_j v_{i+j}\right) \\ =& \sum_{(v_1, \cdots, v_{i-1}, v_{i+1}, \cdots, v_{2i-1}) \in \mathbb{F}_q^{(2i-2)}} \chi\left(\sum_{j=1}^{i-1} v_j v_{i+j}\right) \cdot \sum_{(v_i, v_{2i}) \in \mathbb{F}_q^{(2)}} \chi(v_i v_{2i}) \\ =& q^{i-1} \cdot q = q^i. \end{aligned}$$ □

引理 8.3

$$\sum_{\substack{(v_1,\cdots,v_{2i})\in\mathbb{F}_q^{(2i)}\\ x\neq\sum_{j=1}^{i}v_jv_{i+j}}}\chi(x)=-q^i.$$

证明　实际上,

$$\sum_{\substack{v_1,\cdots,v_{2i},x\in\mathbb{F}_q\\ x\neq\sum_{j=1}^{i}v_jv_{i+j}}}\chi(x)=\sum_{v_1,\cdots,v_{2i},x\in\mathbb{F}_q}\chi(x)-\sum_{\substack{v_1,\cdots,v_{2i},x\in\mathbb{F}_q\\ x=\sum_{j=1}^{i}v_jv_{i+j}}}\chi(x)=0-q^i=-q^i.\quad\square$$

引理 8.4　设 α 是 $\mathbb{F}_q$ 上的一个元素, 且 $\alpha\notin N$. 那么, 我们有

(i) $\sum\limits_{(x,y)\in\mathbb{F}_q^{(2)}}\chi\left(\alpha x^2+xy+\alpha y^2\right)=-q.$

(ii) $\sum\limits_{(v_1,\cdots,v_{2i})\in\mathbb{F}_q^{(2i)}}\chi\Big(\sum\limits_{j=1}^{i-1}v_jv_{i-1+j}+\alpha v_{2i-1}^2+v_{2i-1}v_{2i}+\alpha v_{2i}^2\Big)=-q^i.$

(iii) $\sum\limits_{\substack{(v_1,\cdots,v_{2i})\in\mathbb{F}_q^{(2i)},x\in\mathbb{F}_q,\\ x\neq\sum_{j=1}^{i-1}v_jv_{i+j}+(\alpha v_{2i-1}^2+v_{2i-1}v_{2i}+\alpha v_{2i}^2)}}\chi(x)=q^i,$

证明

$$\sum_{(x,y)\in\mathbb{F}_q^{(2)}}\chi\left(\alpha x^2+xy+\alpha y^2\right)=\sum_{x=0,y\in\mathbb{F}_q}\chi(\alpha y^2)+\sum_{x\neq0,y\in\mathbb{F}_q}\chi\left(\alpha x^2+xy+\alpha y^2\right).$$

注意到右端第一项为 0, 因为当 y 遍及 $\mathbb{F}_q$ 时, y^2 也遍及 $\mathbb{F}_q$. 现在看第二项, 由于 $x\neq0$, 可令 $y=tx$, $t\in\mathbb{F}_q$, 又 $\alpha+t+\alpha t^2\neq0$, $\forall t\in\mathbb{F}_q$. 因此, 我们有

$$\sum_{x\neq0,y\in\mathbb{F}_q}\chi\left(\alpha x^2+xy+\alpha y^2\right)=\sum_{t\in\mathbb{F}_q}\sum_{x\neq0}\chi\left(x^2(\alpha+t+\alpha t^2)\right)=q\cdot(-1)=-q.$$

由引理 8.1 及 (i) 立得 (ii). 仿引理 8.2 的证明可得 (iii).　$\square$

引理 8.5

$$\sum_{\substack{(v_1,\cdots,v_{2i})\in\mathbb{F}_q^{(2i)},\,u\in\mathbb{F}_1^*\\ x+\sum_{j=1}^{i}v_jv_{i+j}\in u^2N}}\chi(x)=\frac{1}{2}q^{i+1}.$$

证明　设 $N=\{a_1=0,a_2,\ldots,a_{q/2}\}$. $x+\sum_{j=1}^{i}v_jv_{i+j}\in u^2N\Leftrightarrow x=\sum_{j=1}^{i}v_jv_{i+j}+u^2a_k$, $k=1,\cdots,q/2$. 因此, 有

$$\sum_{\substack{(v_1,\cdots,v_{2i})\in\mathbb{F}_q^{(2i)},u\in\mathbb{F}_q^*\\ x+\sum_{j=1}^{i}v_jv_{i+j}\in u^2N}}\chi(x)=\sum_{u\in\mathbb{F}_q^*}\sum_{(v_1,\cdots,v_{2i})\in\mathbb{F}_q^{(2i)}}\sum_{k=1}^{q/2}\chi\left(\sum_{j=1}^{i}v_jv_{i+j}+u^2a_k\right)$$

$$=\sum_{k=1}^{q/2}\sum_{u\in\mathbb{F}_q^*}\left(\sum_{(v_1,\cdots,v_{2i})\in\mathbb{F}_q^{(2i)}}\chi\left(\sum_{j=1}^{i}v_jv_{i+j}\right)\right)\chi(u^2a_k)$$

$$=q^i\cdot\sum_{k=1}^{q/2}\sum_{u\in\mathbb{F}_q^*}\chi(u^2a_k)=q^i\cdot\left((q-1)+\left(\frac{q}{2}-1\right)(-1)\right)$$

$$=\frac{1}{2}q^{i+1}.$$

引理 8.6

$$\sum_{\substack{(v_1,\cdots,v_{2i})\in\mathbb{F}_q^{(2i)},\,u\in\mathbb{F}_q^*\\ x+\sum_{j=1}^{i}v_jv_{i+j}\notin u^2N}}\chi(x)=-\frac{1}{2}q^{i+1}.$$

证明 仿引理 8.2 的证明. □

§8.3 二次型的 1 扩充和 $f_r^{(n)}$ 的计算

为了给出非交错对称矩阵对应特征标的递归计算, 我们需要讨论二次型的 1 元扩充, 具体说就是, 设给了一个 $n-1$ 元二次型 A_1, 添加一列得到一个 n 元二次型 A:

$$A_1\equiv\begin{pmatrix}a_{11}&\cdots&a_{1,n-1}\\ &\ddots&\vdots\\ &&a_{n-1,n-1}\end{pmatrix},\quad A\equiv\left(\begin{array}{c|c}A_1&\begin{matrix}x_1\\ \vdots\\ x_{n-1}\end{matrix}\\ \hline 0&x_n\end{array}\right).$$

如果 A_1 是某个型的, 那么 A 的型是怎样变化的, 所添加的元素 $x_1,\cdots,x_n$ 应满足怎样的条件, 所得某种型的 A 之个数是多少? 现在区别 A_1 的型为 $2i^+$, $2i^-$ 和 $2i+1$ 三种情形讨论之.

(1) 设 A_1 的型为 $2i^+(i\geqslant 0)$, 那么存在 $T_1\in Gl_{n-1}(\mathbb{F}_q)$ 使得

$$T_1A_1{}^tT_1\equiv\left[\begin{pmatrix}0&I^{(i)}\\ &0\end{pmatrix},0^{(n-1-2i)}\right].$$

令 $T = T_1 \dotplus (1)$, 那么有

$$TA{}^tT \equiv \left(\begin{array}{ccc|c} 0 & I^{(i)} & & V_1 \\ & 0 & & V_2 \\ & & 0^{(n-1-2i)} & V_3 \\ \hline & & & x_n \end{array}\right), \text{这里} \begin{pmatrix} V_1 \\ V_2 \\ V_3 \end{pmatrix} = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_{n-1} \end{pmatrix} = T_1 \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n-1} \end{pmatrix}. \qquad (8.2)$$

对 $TA{}^tT$ 进一步施行合同变换使得不改 A_1 的型：将 $I^{(i)}$ 所在列右乘以 V_1 加到最后一列, 同时将第 V_2 所在的行左乘以 ${}^tV_1$ 加到最后一行, 然后, 将 $I^{(i)}$ 所在的行左乘以 ${}^tV_2$ 加到最后一行, 同时将第一列右乘以 V_2 加到最后一列. 我们就有

$$TA{}^tT \sim \left(\begin{array}{ccc|c} 0 & I & & 0 \\ & 0 & & V_2 \\ & & 0 & V_3 \\ \hline & & & x_n + {}^tV_1V_2 \end{array}\right) \sim \left(\begin{array}{ccc|c} 0 & I & & 0 \\ & 0 & & 0 \\ & & 0 & V_3 \\ \hline & & & x_n + {}^tV_1V_2 \end{array}\right).$$

于是我们得到下面的论断 (见表 8.1).

表 8.1　A_1 的型为 $2i^+$ 时 A 的情况

A_1 的型	A 的型	添加列满足的条件	A 的个数
$2i^+$	$2i^+$	V_1, V_2 任意, $V_3 = 0$, $x_n = {}^tV_1V_2$	q^{2i}
	$2i+1$	V_1, V_2 任意, $V_3 = 0$, $x_n \neq {}^tV_1V_2$	$q^{2i}(q-1)$
	$2(i+1)^+$	V_1, V_2, x_n 任意, $V_3 \neq 0$	$q^{2i+1}(q^{n-2i-1}-1)$

注：表中给出了 V_1, V_2, V_3 满足的条件, 利用 (8.2) 中的矩阵 T_1 就给出 $x_1, \cdots, x_{n-1}$ 满足的条件.

(2) 设 A_1 的型为 $2i^-(i \geqslant 1)$. 那么存在 $T_1 \in GL_{n-1}(\mathbb{F}_q)$ 使得

$$T_1A_1{}^tT_1 \equiv \left[\begin{pmatrix} 0 & I^{(i-1)} \\ & 0 \end{pmatrix}, \begin{pmatrix} \alpha & 1 \\ & \alpha \end{pmatrix}, 0^{(n-2i-1)}\right].$$

令 $T = T_1 \dotplus (1)$, 那么

$$TA{}^tT \equiv \left(\begin{array}{ccccc|c} 0 & I^{(i-1)} & & & & V_1 \\ & 0 & & & & V_2 \\ & & \alpha & 1 & & v_{2i-1} \\ & & & \alpha & & v_{2i} \\ & & & & 0^{(n-2i-1)} & V_3 \\ \hline & & & & & x_n \end{array}\right),$$

这里

$$\begin{pmatrix} V_1 \\ V_2 \\ v_{2i-1} \\ v_{2i} \\ V_3 \end{pmatrix} = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_{n-1} \end{pmatrix} = T_1 \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n-1} \end{pmatrix}.$$

类似于 (1) 进行合同变换, 可得下面的论断 (见表 8.2).

表 8.2 A_1 的型为 $2i^-$ 时 A 的情况

A_1的型	A 的型	添加列满足的条件	A 的个数
$2i^-$	$2i^-$	$V_1, V_2, v_{2i-1}, v_{2i}$ 任意, $V_3=0$, $x_n = {}^tV_1V_2 + \alpha v_{2i-1}^2 + v_{2i-1}v_{2i} + \alpha v_{2i}^2$	q^{2i}
	$2i+1$	$V_1, V_2, v_{2i-1}, v_{2i}$ 任意, $V_3=0$, $x_n \neq {}^tV_1V_2 + \alpha v_{2i-1}^2 + v_{2i-1}v_{2i} + v_{2i}^2$	$q^{2i}(q-1)$
	$2(i+1)^-$	$V_1, V_2, v_{2i-1}, v_{2i}$, x_n 任意, $V_3 \neq 0$	$q^{2i+1}(q^{n-2i-1}-1)$

(3) 设 A_1 的型为 $2i+1 (i \geqslant 0)$. 这时存在 $T_1 \in GL_{n-1}(\mathbb{F}_q)$ 使得

$$T_1 A_1 {}^tT_1 \equiv \left[\begin{pmatrix} 0 & I^{(i)} \\ & 0 \end{pmatrix}, 1, 0^{(n-2i-2)}\right].$$

令 $T = T_1 \dotplus (1)$, 那么

$$TA\,{}^tT \equiv \left(\begin{array}{cccc|c} 0 & I^{(i)} & & & V_1 \\ & 0 & & & V_2 \\ & & 1 & & v_{2i+1} \\ & & & 0 & V_3 \\ \hline & & & & x_n \end{array}\right), \text{这里} \begin{pmatrix} V_1 \\ V_2 \\ v_{2i+1} \\ V_3 \end{pmatrix} = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_{n-1} \end{pmatrix} = T_1 \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n-1} \end{pmatrix}.$$

类似地进行讨论可得下面的论断 (见表 8.3).

表 8.3 A_1 的型为 $2i+1$ 时 A 的情况

A_1 的型	A 的型	添加列满足的条件	A 的个数
$2i+1$	$2i+1$	V_1, V_2, x_n 任意, $v_{2i+1}=0$, $V_3=0$	q^{2i+1}
	$2(i+1)^+$	V_1, V_2 任意, $v_{2i+1} \neq 0$, $V_3=0$, $x_n + {}^tV_1V_2 \in v_{2i+1}^2 N$	$\frac{1}{2}q^{2i+1}(q-1)$
	$2(i+1)^-$	V_1, V_2 任意, $v_{2i+1} \neq 0$, $V_3=0$, $x_n + {}^tV_1V_2 \notin v_{2i+1}^2 N$	$\frac{1}{2}q^{2i+1}(q-1)$
	$2i+3$	V_1, V_2, v_{2i+1}, x_n 任意, $V_3 \neq 0$	$q^{2i+2}(q^{n-2i-2}-1)$

根据上面的三个论断, 很容易给出各类 n 元二次型个数的递推计数公式, 我们有

定理 8.7 令 $C_i^{(n)}\,(i=0,1,2^+,2^-,3,\cdots)$ 表示型为 i 的 n 元二次型的集合, 那么有

(i) $|C_{2i^+}^{(n)}|=q^{2i}|C_{2i^+}^{(n-1)}|+\frac{1}{2}q^{2i-1}(q-1)|C_{2i-1}^{(n-1)}|+q^{2i-1}(q^{n-2i+1}-1)|C_{2(i-1)^+}^{(n-1)}|$.

(ii) $|C_{2i^-}^{(n)}|=q^{2i}|C_{2i^-}^{(n-1)}|+\frac{1}{2}q^{2i-1}(q-1)|C_{2i-1}^{(n-1)}|+q^{2i-1}(q^{n-2i+1}-1)|C_{2(i-1)^-}^{(n-1)}|$.

(iii) $|C_{2i+1}^{(n)}|=q^{2i+1}|C_{2i+1}^{(n-1)}|+q^{2i}(q-1)|C_{2i^+}^{(n-1)}|+q^{2i}(q-1)|C_{2i^-}^{(n-1)}|+q^{2i}(q^{n-2i}-1)|C_{2i-1}^{(n-1)}|$.

注意: 在本文涉及到的计数公式中, 如果 $k>n$, 则约定 $C_k^{(n)}=\varnothing$.

证明 看 (i). 设 A 是一个型为 $2i^+$ 的 n 元二次型. 由上述论断知, 它的左上角 $n-1$ 元二次型 A_1 的类型有三种可能, 即 $2i^+$, $2i-1$ 和 $2(i-1)^+$. 当 A_1 取为 $2i^+$ 型的时, 可以得到 q^{2i} 个 $2i^+$ 型的 A; 当 A_1 取为 $2i-1$ 型的时, 可以得到 $\frac{1}{2}q^{2i-1}(q-1)$ 个 $2i^+$ 的 A; 当 A_1‘ 取为 $2(i-1)^+$ 型的时, 可以得到 $q^{2i-1}(q^{n-2i+1}-1)$ 个 $2i^+$ 型的 A. 并且每个 $2i^+$ 型的 n 元二次型 A 均可如此得到, 所以我们就有 (i) 成立.

同理可得到 (ii) 和 (iii). □

利用定理 8.7 中给出的关于 $|C_k^{(n)}|$ 的递推公式可以得到秩为 $r<n$ 的非交错对称矩阵对应特征标 $f_r^{(n)}$ 给出的特征值之递推计算公式. 我们有

定理 8.8 秩为 $0<r<n$ 非交错对称矩阵对应特征标 $f_r^{(n)}$ 给出的特征值满足下面的等式

(i)
$$f_r^{(n)}(C_{2i^+}^{(n)})=q^{2i}f_r^{(n-1)}(C_{2i^+}^{(n-1)})+\frac{1}{2}q^{2i-1}(q-1)f_r^{(n-1)}(C_{2i-1}^{(n-1)})+q^{2i-1}(q^{n-2i+1}-1)f_r^{(n-1)}(C_{2(i-1)^+}^{(n-1)}).$$

(ii)
$$f_r^{(n)}(C_{2i^-}^{(n)})=q^{2i}f_r^{(n-1)}(C_{2i^-}^{(n-1)})+\frac{1}{2}q^{2i-1}(q-1)f_r^{(n-1)}(C_{2i-1}^{(n-1)})+q^{2i-1}(q^{n-2i+1}-1)f_r^{(n-1)}(C_{2(i-1)^-}^{(n-1)}).$$

(iii)
$$f_r^{(n)}(C_{2i+1}^{(n)})=q^{2i+1}f_r^{(n-1)}(C_{2i+1}^{(n-1)})+q^{2i}(q-1)f_r^{(n-1)}(C_{2i^+}^{(n-1)})+q^{2i}(q-1)f_r^{(n-1)}(C_{2i^-}^{(n-1)})+q^{2i}(q^{n-2i}-1)f_r^{(n-1)}(C_{2i-1}^{(n-1)}).$$

证明 由定理 8.7 立得. □

我们还需要满秩非交错对称矩阵对应特征标给出的特征值的算法.

定理 8.9 对于秩为 n 的非交错对称矩阵对应特征标 $f_n^{(n)}$, 我们有

(i) $f_n^{(n)}(C_{2i^+}^{(n)})=q^if_{n-1}^{(n-1)}(C_{2i^+}^{(n-1)})+\frac{1}{2}q^if_{n-1}^{(n-1)}(C_{2i-1}^{(n-1)})$.

(ii) $f_n^{(n)}(C_{2i^-}^{(n)})=-q^if_{n-1}^{(n-1)}(C_{2i^-}^{(n-1)})-\frac{1}{2}q^if_{n-1}^{(n-1)}(C_{2i-1}^{(n-1)})$.

(iii) $f_n^{(n)}(C_{2i+1}^{(n)})=-q^if_{n-1}^{(n-1)}(C_{2i^+}^{(n-1)})+q^if_{n-1}^{(n-1)}(C_{2i^-}^{(n-1)})$.

证明 (i) 从上面的三条论断可知, $C_{2i^+}^{(n)}$ 由三部分元素组成, 第一部分是那些

左上角 A_1 为 $2i^+$ 型的元素, 对于每个 $2i^+$ 型的 A_1, 有 q^{2i} 个型为 $2i^+$ 的 1 扩充 A, $f_n^{(n)}$ 在每个这样的 A 处取值为 $f_n^{(n)}(A) = f_{n-1}^{(n-1)}(A_1)\chi(x_n)$, 其中 $x_n = \sum_{j=1}^{i} v_j v_{i+j}$. 因此, 第一部分元素对于 $f_n^{(n)}(C_{2i^+}^{(n)})$ 的贡献为

$$\sum_{\substack{(v_1,\cdots,v_{2i})\in\mathbb{F}_q^{(2i)},\\ x_n=\sum_{j=0}^{i} v_j v_{i+j},(v_{2i+1}\cdots v_{n-1})=0}} \chi(x_n)\cdot f_{n-1}^{(n-1)}(C_{2i^+}^{(n-1)}).$$

同理, 考虑第二部分元素, 它是那些左上角 A_1 为 $2i-1$ 型的 $n-1$ 元二次型的 1 扩充, 再考虑第三部分元素, 它是那些左上角 A_1 为 $2(i-1)^+$ 型的 1 扩充, 对于这两部分元素也考虑它们对 $f_n^{(n)}(C_{2i^+}^{(n)})$ 的贡献, 就可得

$$\begin{aligned} f_n^{(n)}(C_{2i^+}^{(n)}) = & \sum_{\substack{(v_1,\ldots,v_{2i})\in\mathbb{F}_q^{(2i)},\\ x_n=\sum_{j=1}^{i} v_j v_{i+j},(v_{2i+1},\ldots,v_{n-1})=0}} \chi(x_n)\cdot f_{n-1}^{(n-1)}(C_{2i^+}^{(n-1)}) \\ & + \sum_{\substack{(v_1,\ldots,v_{2i-2})\in\mathbb{F}_q^{(2i-2)},\ v_{2i-1}\neq 0,\\ x_n+\sum_{j=1}^{i-1} v_j v_{i+j}\in v_{2i-1}^2 N,(v_{2i},\ldots,v_{n-1})=0}} \chi(x_n)\cdot f_{n-1}^{(n-1)}(C_{2i-1}^{(n-1)}) \\ & + \sum_{\substack{(v_1,\ldots,v_{2i-2})\in\mathbb{F}_q^{(2i-2)},\\ x_n+\sum_{j=1}^{i-1} v_j v_{i-1+j}\text{任意},\ (v_{2i-1},\cdots,v_{n-1})\neq 0}} \chi(x_n)\cdot f_{n-1}^{(n-1)}(C_{2(i-1)^+}^{(n-1)}). \end{aligned}$$

由引理 8.2, 引理 8.5 和引理 8.1 立得等式 (i).

类似地可得 (ii) 和 (iii). □

定理 8.10 对于 $f_r^{(n)}$ 在 $C_1^{(n)}$ 上的取值, 我们有

$$f_r^{(n)}(C_1^{(n)}) = -1, \quad r = 1, 2, \ldots, n.$$

证明 如果 $r = n$, 那么由定理 8.9(iii), 立得 $f_n^{(n)}(C_1^{(n)}) = -1$. 设 $r < n$, 由定理 8.8(iii), 有

$$f_r^{(n)}(C_1^{(n)}) = q f_r^{(n-1)}(C_1^{(n-1)}) + (q-1).$$

对 n 作归纳法立得. □

定理 8.8～ 定理 8.10 实际上给出了非交错对称矩阵对应特征标在类 $C_k^{(n)}$ 上取值 (即二次型方案的某些特征值) 的递推计算方法. §8.8 中 $n=3$ 时的特征值我们曾用列出各类 3 元二次型的办法具体计算出来, 后来用定理 8.8 和定理 8.9 的方法又进行了计算, 结果是完全一致的. 接着我们又用这种方法计算出 $n=4$ 时 $f_r^{(4)}$ 给出的特征值.

§8.4 $f_r^{(n)}$ 在合并类 $C_{2i}^{(n)}$ 上的取值

对于二次型的合并类 $C_{2i+}^{(n)}$ 和 $C_{2i-}^{(n)}(i>0)$, 令 $C_{2i}^{(n)}$ 表示二者的并. 这样, $C_k^{(n)}(k=0,1,\cdots,n)$ 表示秩为 k 的 n 元二次型的集合. 再令 $f_r^{(n)}(C_k^{(n)})=\sum_{X\in C_k^{(n)}} f_r^{(n)}(X)$, 特别是

$$f_r^{(n)}(C_{2i}^{(n)})=f_r^{(n)}(C_{2i+}^{(n)})+f_r^{(n)}(C_{2i-}^{(n)}).$$

定理 8.11 对于非交错对称矩阵对应特征标 $f_r^{(n)}$, 恒有

$$f_r^{(n)}(C_{2i+1}^{(n)})+f_r^{(n)}(C_{2i}^{(n)})=0,\ \ (i=0,1,\cdots,[\frac{n}{2}];r=1,2,\cdots,n).$$

证明 由 §8.8 可知, 这个论断对于 $n=2,3,4$ 都成立. 今用归纳法证明对每个 n 都成立. 设 $n\geqslant 5$, 并且假设对于不超过 $n-1$ 元的二次型来说上述论断成立, 往证对于 n 元二次型也成立.

先设 $r<n$. 这时由定理 8.8 的 (i), (ii) 和 (iii), 我们有

$$\begin{aligned}f_r^{(n)}(C_{2i}^{(n)})=&\ q^{2i}f_r^{(n-1)}(C_{2i}^{(n-1)})+(q^{2i}-q^{2i-1})f_r^{(n-1)}(C_{2i-1}^{(n-1)})\\&+(q^n-q^{2i-1})f_r^{(n-1)}(C_{2i-2}^{(n-1)}),\\f_r^{(n)}(C_{2i+1}^{(n)})=&\,q^{2i+1}f_r^{(n-1)}(C_{2i+1}^{(n-1)})+(q^{2i+1}-q^{2i})f_r^{(n-1)}(C_{2i}^{(n-1)})\\&+(q^n-q^{2i})f_r^{(n-1)}(C_{2i-1}^{(n-1)}).\end{aligned}$$

于是有

$$\begin{aligned}f_r^{(n)}(C_{2i+1}^{(n)})+f_r^{(n)}(C_{2i}^{(n)})=&\,q^{2i+1}\{f_r^{(n-1)}(C_{2i+1}^{(n-1)})+f_r^{(n-1)}(C_{2i}^{(n-1)})\}\\&+(q^n-q^{2i-1})\{f_r^{(n-1)}(C_{2i-1}^{(n-1)})+f_r^{(n-1)}(C_{2i-2}^{(n-1)})\}.\end{aligned}$$

依归纳假设, 等式右端两个括号中之和均为 0, 因此右端结果为 0.

现在设 $r=n$. 这时由定理 8.9 的 (i), (ii) 和 (iii) 相加立得

$$f_n^{(n)}(C_{2i}^{(n)})+f_n^{(n)}(C_{2i+1}^{(n)})=0.\qquad\square$$

由定理 8.11 可知, 我们只需计算 $f_r^{(n)}$ 在 $C_{2i}^{(n)}(i=1,\cdots,[\frac{n}{2}])$ 上的取值就够了.

定理 8.12

(i) 对于 $1\leqslant r<n$, 我们有

$$f_r^{(n)}(C_{2i}^{(n)})=q^{2i}f_r^{(n-1)}(C_{2i}^{(n-1)})+(q^n-q^{2i})f_r^{(n-1)}(C_{2i-2}^{(n-1)}).$$

(ii) $f_n^{(n)}(C_{2i}^{(n)})=q^{2i}f_{n-2}^{(n-2)}(C_{2i}^{(n-2)})-q^{2i}f_{n-2}^{(n-2)}(C_{2i-2}^{(n-2)})\ (2i<n)$.

(iii) 如果 n 为偶数, 比方设 $n=2m$, 则有

$$f_r^{(2m)}(C_{2m}^{(2m)})=0.\ r=1,\ 2,\ \cdots,\ 2m.$$

证明 (i) 由定理 8.8 的 (i), (ii) 和定理 8.11 立得.

(ii) 由定理 8.9 的 (i), (ii), 得

$$f_n^{(n)}(C_{2i}^{(n)})=q^i\{f_{n-1}^{(n-1)}(C_{2i^+}^{(n-1)})-f_{n-1}^{(n-1)}(C_{2i^-}^{(n-1)})\}. \tag{8.3}$$

再用一次定理 8.9 的 (i), (ii), 而将 n 换成 $n-1$, 可得

$$f_{n-1}^{(n-1)}(C_{2i^+}^{(n-1)})-f_{n-1}^{(n-1)}(C_{2i^-}^{(n-1)})=q^if_{n-2}^{(n-2)}(C_{2i}^{(n-2)})+q^if_{n-2}^{(n-2)}(C_{2i-1}^{(n-2)}).$$

于是

$$f_n^{(n)}(C_{2i}^{(n)})=q^{2i}f_{n-2}^{(n-2)}(C_{2i}^{(n-2)})+q^{2i}f_{n-2}^{(n-2)}(C_{2i-1}^{(n-2)}).$$

由定理 8.11, 将 $f_{n-2}^{(n-2)}(C_{2i-1}^{(n-2)})$ 换成 $-f_{n-2}^{(n-2)}(C_{2i-2}^{(n-2)})$, 即得所要结果.

(iii) 设 $n=2m$. 如果 $r<2m$, 那么由 (i) 知 $f_r^{(2m)}(C_{2m}^{(2m)})=0$. 如果 $r=n$, 那么由定理 8.9(i) (ii), 可得 $f_{2m}^{(2m)}(C_{2m}^{(2m)})=0$. □

对于非交错对称矩阵给出的特征标 $f_r^{(n)}$, 还有下面的性质

定理 8.13 $f_{2k}^{(n)}$ 和 $f_{2k-1}^{(n)}$ 在每个类 $C_j^{(n)}$ 上取值相同, 即

$$f_{2k}^{(n)}(C_j^{(n)})=f_{2k-1}^{(n)}(C_j^{(n)}),\ j=0,\ 1,\ \cdots,\ n;\quad k=1,\ \cdots,\ \left[\frac{n}{2}\right].$$

证明 由定理 8.11, 我们只需考虑 j 为偶数的类就可以了. 当 $j=0$ 时, 结论显然. 下面设 $j=2i$, $i>0$. 现在对 n 施行归纳法.

当 $n=2,\ 3,\ 4$ 时, 由 §8.8 可知结论成立. 设 $n\geqslant 5$, 并且假设对于不超过 $n-1$ 元的二次型来说上述结论成立, 往证对于 n 元的二次型上述结论亦成立.

先看 $2k<n$ 的情形, 这时由定理 8.12(i) 有

$$f_{2k}^{(n)}(C_{2i}^{(n)})=q^{2i}f_{2k}^{(n-1)}(C_{2i}^{(n-1)})+(q^n-q^{2i})f_{2k}^{(n-1)}(C_{2i-2}^{(n-1)}),$$
$$f_{2k-1}^{(n)}(C_{2i}^{(n)})=q^{2i}f_{2k-1}^{(n-1)}(C_{2i}^{(n-1)})+(q^n-q^{2i})f_{2k-1}^{(n-1)}(C_{2i-2}^{(n-1)}).$$

由归纳假设, $f_{2k}^{(n-1)}(C_{2i}^{(n-1)})=f_{2k-1}^{(n-1)}(C_{2i}^{(n-1)})$, $f_{2k}^{(n-1)}(C_{2i-2}^{(n-1)})=f_{2k-1}^{(n-1)}(C_{2i-2}^{(n-1)})$, 故有 $f_{2k}^{(n)}(C_{2i}^{(n)})=f_{2k-1}^{(n)}(C_{2i}^{(n)})$.

如果 $2k+1=n$, 那么就通过了. 现在设 $n=2m$, 那么尚需证明对于 $f_{2m}^{(2m)}$ 和 $f_{2m-1}^{(2m)}$ 上述结论成立.

由定理 8.12(ii), 我们有

$$
\begin{aligned}
& f_{2m}^{(2m)}(C_{2i}^{(2m)}) \\
={} & q^{2i} f_{2m-2}^{(2m-2)}(C_{2i}^{(2m-2)}) - q^{2i} f_{2m-2}^{(2m-2)}(C_{2i-2}^{(2m-2)}) \\
={} & q^{2i} f_{2m-3}^{(2m-2)}(C_{2i}^{(2m-2)}) - q^{2i} f_{2m-3}^{(2m-2)}(C_{2i-2}^{(2m-2)}) \quad (\text{由归纳假设}) \\
={} & q^{2i}\{q^{2i} f_{2m-3}^{(2m-3)}(C_{2i}^{(2m-3)}) + (q^{2m-2} - q^{2i}) f_{2m-3}^{(2m-3)}(C_{2i-2}^{(2m-3)})\} \\
& - q^{2i}\{q^{2i-2} f_{2m-3}^{(2m-3)}(C_{2i-2}^{(2m-3)}) + (q^{2m-2} - q^{2i-2}) f_{2m-3}^{(2m-3)}(C_{2i-4}^{(2m-3)})\}, \\
& \hfill (\text{由定理 } 8.12(\text{i})) \\
={} & q^{4i} f_{2m-3}^{(2m-3)}(C_{2i}^{(2m-3)}) + (q^{2m+2i-2} - q^{4i} - q^{4i-2}) f_{2m-3}^{(2m-3)}(C_{2i-2}^{(2m-3)}) \\
& - (q^{2m+2i-2} - q^{4i-2}) f_{2m-3}^{(2m-3)}(C_{2i-4}^{(2m-3)}).
\end{aligned}
$$

另一方面, 由定理 8.12(i), 有

$$
\begin{aligned}
& f_{2m-1}^{(2m)}(C_{2i}^{(2m)}) \\
={} & q^{2i} f_{2m-1}^{(2m-1)}(C_{2i}^{(2m-1)}) + (q^{2m} - q^{2i}) f_{2m-1}^{(2m-1)}(C_{2i-2}^{(2m-1)}) \\
={} & q^{2i} q^{i}\{f_{2m-2}^{(2m-2)}(C_{2i^+}^{(2m-2)}) - f_{2m-2}^{(2m-2)}(C_{2i^-}^{(2m-2)})\} \\
& + (q^{2m} - q^{2i}) q^{i-1}\{f_{2m-2}^{(2m-2)}(C_{2(i-1)^+}^{(2m-2)}) - f_{2m-2}^{(2m-2)}(C_{2(i-1)^-}^{(2m-2)})\} (\text{由 } (8.3) \text{ 式}) \\
={} & q^{3i}\{q^{i} f_{2m-3}^{(2m-3)}(C_{2i}^{(2m-3)}) + q^{i} f_{2m-3}^{(2m-3)}(C_{2i-1}^{(2m-3)})\} \\
& + (q^{2m} - q^{2i}) q^{i-1}\{q^{i-1} f_{2m-3}^{(2m-3)}(C_{2i-2}^{(2m-3)}) + q^{i-1} f_{2m-3}^{(2m-3)}(C_{2m-3}^{(2m-3)})\} \\
={} & q^{4i} f_{2m-3}^{(2m-3)}(C_{2i}^{(2m-3)}) + (q^{2m+2i-2} - q^{4i-2} - q^{4i}) f_{2m-3}^{(2m-3)}(C_{2i-2}^{(2m-3)}) \\
& - (q^{2m+2i-2} - q^{4i-2}) f_{2m-3}^{(2m-3)}(C_{2i-4}^{(2m-3)}). (\text{由定理}8.11)
\end{aligned}
$$

于是立得所需结论. □

§8.5　二次型的 2 扩充和 $f_{2k^*}^{(n)}$ 的计算

为了给出交错矩阵对应特征标的递推计算, 我们需要讨论二次型的 2 元扩充. 就是说, 设给了一个 $n-2$ 元的二次型 A_1, 添加两列得到 n 元二次型 A:

$$
A_1 \equiv \begin{pmatrix} a_{11} & \cdots & a_{1,n-2} \\ & \ddots & \vdots \\ & & a_{n-2,n-2} \end{pmatrix} \text{ 和 } A \equiv \left(\begin{array}{c|cc} & x_{11} & x_{12} \\ A_1 & \vdots & \vdots \\ & x_{n-2,1} & x_{n-2,2} \\ \hline & a & b \\ & & c \end{array}\right).
$$

我们分别就 A_1 的各种类型讨论 A 可能的类型, 并确定所添加元素的关系, 以及各类型 A 的计数. A 的类型有时用 $t(A)$ 表示.

(I) 设 $t(A_1) = 2i^+ \ (i \geqslant 0)$. 那么存在 $T_1 \in GL_{n-2}(\mathbb{F}_q)$, 使得

$$T_1 A_1 {}^t T_1 \equiv \left[\begin{pmatrix} 0 & I^{(i)} \\ & 0 \end{pmatrix}, 0^{(n-2i-2)} \right].$$

设 $T = T_1 \dot{+} I^{(2)}$, 那么有

$$TA{}^tT \equiv \left(\begin{array}{ccc|cc} 0 & I^{(i)} & & V_{11} & V_{12} \\ & 0 & & V_{21} & V_{22} \\ & & 0^{(n-2i-2)} & V_{31} & V_{32} \\ \hline & & & a & b \\ & & & & c \end{array} \right),$$

这里

$$\begin{pmatrix} V_{11} & V_{12} \\ V_{21} & V_{22} \\ V_{31} & V_{32} \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} \\ \vdots & \vdots \\ v_{n-2,1} & v_{n-2,2} \end{pmatrix} = T_1 \begin{pmatrix} x_{11} & x_{12} \\ \vdots & \vdots \\ x_{n-2,1} & x_{n-2,2} \end{pmatrix}.$$

仿 §8.3 中的讨论我们首先有

$$TA{}^tT \sim \left[\begin{pmatrix} 0 & I^{(i)} \\ & 0 \end{pmatrix}, \left(\begin{array}{c|cc} 0^{(n-2i-2)} & V_{31} & V_{32} \\ \hline & a' & b' \\ & & c' \end{array} \right) \right],$$

这里

$$\begin{aligned} a' &= a + {}^tV_{11} V_{21}, \\ b' &= b + {}^tV_{12}V_{21} + {}^tV_{11}V_{22}, \quad V_{11}, V_{12}, V_{21}, V_{22} \text{ 可任取}. \\ c' &= c + {}^tV_{12}V_{22}. \end{aligned}$$

再区分 $\mathrm{rank}(V_{31}\ V_{32}) = 0, 1, 2$ 讨论之.

(Ia) 设 $(V_{31}\ V_{32}) = 0$,

$$A \sim \left[\begin{pmatrix} 0 & I^{(i)} \\ & 0 \end{pmatrix}, 0^{(n-2i-2)}, \begin{pmatrix} a' & b' \\ & c' \end{pmatrix} \right].$$

我们得到的结论见表 8.4.

表 8.4 A 的型及相应的情况

A 的型	添加列满足的条件	A 的个数
$2i^+$	$V_{11}, V_{12}, V_{21}, V_{22}$ 任意, $V_{31} = V_{32} = 0$, $a' = b' = c' = 0$	q^{4i}
$2i+1$	$V_{11}, V_{12}, V_{21}, V_{22}$ 任意, $V_{31} = V_{32} = 0$, $b' = 0, (a', c') \neq 0$	$q^{4i}(q^2-1)$
$2(i+1)^+$	$V_{11}, V_{12}, V_{21}, V_{22}$ 任意, $V_{31} = V_{32} = 0$, $b' \neq 0, a'c' \in b'^2 N$	$\frac{1}{2}q^{4i+1}(q^2-1)$
$2(i+1)^-$	$V_{11}, V_{12}, V_{21}, V_{22}$ 任意, $V_{31} = V_{32} = 0$, $b' \neq 0, a'c' \notin b'^2 N$	$\frac{1}{2}q^{4i+1}(q-1)^2$

(Ib) $\mathrm{rank}(V_{31}\ V_{32})=1$. 这时

$$A\sim\left(\begin{array}{cccc|cc} 0 & I^{(i)} & & & 0 & 0\\ & 0 & & & 0 & 0\\ & & 0^{(n-2i-3)} & & 0 & 0\\ & & & 0 & u & v\\ \hline & & & & a' & b'\\ & & & & & c' \end{array}\right),$$

且 $(u,v)\neq 0$. (秩为 1 的 $(n-2i-2)\times 2$ 矩阵个数为 $(q+1)(q^{n-2i-2}-1)$.) 进一步可知有如下论断 (见表 8.5).

表 8.5 A 的型及相应的情况

A 的型	添加列满足的条件	A 的个数
$2i+3$	$V_{11},V_{12},V_{21},V_{22},a',b'$ 任意, $v=0$, $u\neq 0,c'\neq 0$, $\mathrm{rank}(V_{31}\,V_{32})=1$	$q^{4i+2}(q^{n-2i-2}-1)(q-1)$
$2i+3$	$V_{11},V_{12},V_{21},V_{22},u,b',c'$ 任意, $v\neq 0$, $a'\neq v^{-1}ub'+v^{-2}u^2c'$, $\mathrm{rank}(V_{31}\,V_{32})=1$	$q^{4i+3}(q^{n-2i-2}-1)(q-1)$
$2(i+1)^+$	$V_{11},V_{12},V_{21},V_{22},a',b'$ 任意, $v=0$, $u\neq 0,c'=0$, $\mathrm{rank}(V_{31}\,V_{32})=1$	$q^{4i+2}(q^{n-2i-2}-1)$
$2(i+1)^+$	$V_{11},V_{12},V_{21},V_{22},u,b',c'$ 任意, $v\neq 0$, $a'=v^{-1}ub'+v^{-2}u^2c'$, $\mathrm{rank}(V_{31}\,V_{32})=1$	$q^{4i+3}(q^{n-2i-2}-1)$

(Ic) $\mathrm{rank}(V_{31}\ V_{32})=2\ \ (n-2i-2\geqslant 2)$. 这时

$$A\sim\left[\begin{pmatrix}0 & I^{(i)}\\ & 0\end{pmatrix},0^{(n-2i-4)},\begin{pmatrix}0 & 0 & 1 & 0\\ & 0 & 0 & 1\\ & & a' & b'\\ & & & c'\end{pmatrix}\right].$$

我们有如下论断 (见表 8.6).

表 8.6 A 的型及相应的情况

A 的型	添加列满足的条件	A 的个数
$2(i+2)^+$	$V_{11},V_{12},V_{21},V_{22},a',b',c'$ 任意, $\mathrm{rank}(V_{31}\,V_{32})=2$,	$q^{4i+4}(q^{n-2i-2}-1)(q^{n-2i-3}-1)$

(II) 设 $t(A_1)=2i^-(i\geqslant 1)$. 那么存在 $T_1\in GL_{n-2}(\mathbb{F}_q)$, 使得

$$T_1A_1\,{}^tT_1\equiv\left[\begin{pmatrix}0 & I^{(i-1)}\\ & 0\end{pmatrix},\begin{pmatrix}\alpha & 1\\ & \alpha\end{pmatrix},0^{(n-2i-2)}\right].$$

令 $T = T_1 + I^{(2)}$. 那么

$$TA{}^tT \equiv \left(\begin{array}{ccccc|cc} 0 & I^{(i-1)} & & & & V_{11} & V_{12} \\ & 0 & & & & V_{21} & V_{22} \\ & & \alpha & 1 & & w_{11} & w_{12} \\ & & & \alpha & & w_{21} & w_{22} \\ & & & & 0^{(n-2i-2)} & V_{31} & V_{32} \\ \hline & & & & & a & b \\ & & & & & & c \end{array}\right),$$

这里

$$\begin{pmatrix} V_{11} & V_{12} \\ V_{21} & V_{22} \\ w_{11} & w_{12} \\ w_{21} & w_{22} \\ V_{31} & V_{32} \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} \\ \vdots & \vdots \\ v_{n-2,1} & v_{n-2,2} \end{pmatrix} = T_1 \begin{pmatrix} x_{11} & x_{12} \\ \vdots & \vdots \\ x_{n-2,1} & x_{n-2,2} \end{pmatrix}.$$

仿 8.3 中的讨论我们有

$$TA{}^tT \sim \begin{pmatrix} 0 & I^{(i-1)} & & & & 0 & 0 \\ & 0 & & & & 0 & 0 \\ & & \alpha & 1 & & 0 & 0 \\ & & & \alpha & & 0 & 0 \\ & & & & 0^{(n-2i-2)} & V_{31} & V_{32} \\ & & & & & a' & b' \\ & & & & & & c' \end{pmatrix},$$

这里

$$a' = a + {}^tV_{11}V_{21} + \alpha w_{11}^2 + w_{11}w_{21} + \alpha w_{21}^2,$$
$$b' = b + {}^tV_{12}V_{21} + {}^tV_{11}V_{22} + w_{11}w_{22} + w_{12}w_{21},$$
$$c' = c + {}^tV_{12}V_{22} + \alpha w_{12}^2 + w_{12}w_{22} + \alpha w_{22}^2.$$

(IIa) 设 $(V_{31}\ V_{32}) = 0$. 则

$$A \sim \left[\begin{pmatrix} 0 & I^{(i-1)} \\ & 0 \end{pmatrix}, \begin{pmatrix} \alpha & 1 \\ & \alpha \end{pmatrix}, 0^{(n-2i-2)}, \begin{pmatrix} a' & b' \\ & c' \end{pmatrix}\right].$$

我们有如下论断 (见表 8.7).

表 8.7　A 的型及相应的情况

A 的型	添加列满足的条件	A 的个数
$2i^-$	$V_{11}, V_{12}, V_{21}, V_{22}, w_{11}, w_{12}, w_{21}, w_{22}$ 任意, $V_{31} = V_{32} = 0,\ a' = b' = c' = 0$	q^{4i}
$2i+1$	$V_{11}, V_{12}, V_{21}, V_{22}, w_{11}, w_{12}, w_{21}, w_{22}$ 任意, $V_{31} = V_{32} = 0,\ b' = 0, (a', c') \neq 0$	$q^{4i}(q^2-1)$
$2(i+1)^+$	$V_{11}, V_{12}, V_{21}, V_{22}, w_{11}, w_{12}, w_{21}, w_{22}$ 任意, $V_{31} = V_{32} = 0,\ b' \neq 0,\ a'c' \notin b'^2 N$	$\frac{1}{2}q^{4i+1}(q-1)^2$
$2(i+1)^-$	$V_{11}, V_{12}, V_{21}, V_{22}, w_{11}, w_{12}, w_{21}, w_{22}$ 任意, $V_{31} = V_{32} = 0,\ b' \neq 0,\ a'c' \in b'^2 N$	$\frac{1}{2}q^{4i+1}(q^2-1)$

(IIb) 设 $\mathrm{rank}(V_{31}V_{32}) = 1$, 这时

$$A \sim \left[\begin{pmatrix} 0 & I^{(i-1)} \\ & 0 \end{pmatrix}, \begin{pmatrix} \alpha & 1 \\ & \alpha \end{pmatrix}, 0^{(n-2i-3)}, \begin{pmatrix} 0 & u & v \\ & a' & b' \\ & & c' \end{pmatrix}\right], \text{ 且}(u, v) \neq 0.$$

我们有如下论断 (见表 8.8).

表 8.8　A 的型及相应的情况

A 的型	添加列满足的条件	A 的个数
$2i+3$	$V_{11}, V_{12}, V_{21}, V_{22}, w_{11}, w_{12}, w_{21}, w_{22}$, a', b' 任意, $c \neq 0, u \neq 0, v = 0$, $\mathrm{rank}(V_{31}\ V_{32}) = 1$	$q^{4i+2}(q^{n-2i-2}-1)(q-1)$
$2i+3$	$V_{11}, V_{12}, V_{21}, V_{22}, w_{11}, w_{12}, w_{21}, w_{22}, b'$, c', u 任意, $v \neq 0,\ a' \neq v^{-1}ub' + v^{-2}u^2c'$, $\mathrm{rank}(V_{31}\ V_{32}) = 1$	$q^{4i+3}(q^{n-2i-2}-1)(q-1)$
$2(i+1)^-$	$V_{11}, V_{12}, V_{21}, V_{22}, w_{11}, w_{12}, w_{21}, w_{22}$, a', b' 任意, $c = 0, v = 0, u \neq 0$, $\mathrm{rank}(V_{31}\ V_{32}) = 1$	$q^{4i+2}(q^{n-2i-2}-1)$
$2(i+1)^-$	$V_{11}, V_{12}, V_{21}, V_{22}, w_{11}, w_{12}, w_{21}, w_{22}, b'$, c', u 任意, $v \neq 0, a' = v^{-1}ub' + v^{-2}u^2c'$, $\mathrm{rank}(V_{31}\ V_{32}) = 1$	$q^{4i+3}(q^{n-2i-2}-1)$

(IIc) 设 $\mathrm{rank}(V_{31}\ V_{32}) = 2\ (n-2i-2 \geqslant 2)$. 这时

$$A \sim \left[\begin{pmatrix} 0 & I^{(i-1)} \\ & 0 \end{pmatrix}, \begin{pmatrix} \alpha & 1 \\ & \alpha \end{pmatrix}, 0^{(n-2i-4)}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ & 0 & 0 & 1 \\ & & a' & b' \\ & & & c' \end{pmatrix}\right].$$

我们有如下论断 (见表 8.9).

表 8.9 A 的型及相应的情况

A 的型	添加列满足的条件	A 的个数
$2(i+2)^-$	$V_{11}, V_{12}, V_{21}, V_{22}, a', b', c', w_{11}, w_{12}, w_{21}, w_{22}$ 任意, $\text{rank}(V_{31}\, V_{32}) = 2$	$q^{4i+4}(q^{n-2i-2}-1)(q^{n-2i-3}-1)$

(III) 设 $t(A_1) = 2i+1$. 那么存在 $T_1 \in GL_{n-2}(\mathbb{F}_q)$. 使得

$$T_1 A_1 {}^t T_1 \equiv \begin{pmatrix} 0 & I^{(i)} & & \\ & 0 & & \\ & & 1 & \\ & & & 0^{(n-2i-3)} \end{pmatrix}.$$

令 $T = T_1 \dotplus I^{(2)}$. 那么有

$$TA{}^tT \equiv \left(\begin{array}{cccc|cc} 0 & I^{(i)} & & & V_{11} & V_{12} \\ & 0 & & & V_{21} & V_{22} \\ & & 1 & & w_1 & w_2 \\ & & & 0^{(n-2i-3)} & V_{31} & V_{32} \\ & & & & a & b \\ \hline & & & & & c \end{array}\right),$$

这里

$$\begin{pmatrix} V_{11} & V_{12} \\ V_{21} & V_{22} \\ w_1 & w_2 \\ V_{31} & V_{32} \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} \\ \vdots & \vdots \\ v_{n-2,1} & v_{n-2,2} \end{pmatrix} = T_1 \begin{pmatrix} x_{11} & x_{12} \\ \vdots & \vdots \\ x_{n-2,1} & x_{n-2,2} \end{pmatrix}.$$

仿 8.3 中的讨论我们有

$$TA{}^tT \sim \begin{pmatrix} 0 & I^{(i)} & & & 0 & 0 \\ & 0 & & & 0 & 0 \\ & & 1 & & w_1 & w_2 \\ & & & 0^{(n-2i-3)} & V_{31} & V_{32} \\ & & & & a' & b' \\ & & & & & c' \end{pmatrix},$$

这里

$$\begin{aligned} a' &= a + {}^tV_{11}V_{21}, \\ b' &= b + {}^tV_{11}V_{22} + {}^tV_{12}V_{21}, \\ c' &= c + {}^tV_{12}V_{22}. \end{aligned}$$

区别以下情形讨论之.

(IIIa) $(V_{31}\,V_{32}) = 0$. 又分以下两种情形

(IIIa1) 如果 $(w_1,\,w_2) = 0$, 那么有如下论断 (见表 8.10).

表 8.10 A 的型及相应的情况

A 的型	添加列满足的条件	A 的个数
$2i+1$	$V_{11}, V_{12}, V_{21}, V_{22}, a', c'$ 任意, $b' = 0$, $V_{31} = V_{32} = 0$	q^{4i+2}
$2i+3$	$V_{11}, V_{12}, V_{21}, V_{22}, a', c'$ 任意, $b' \neq 0$, $V_{31} = V_{32} = 0$	$q^{4i+2}(q-1)$

(IIIa2) 如果 $(w_1,\,w_2) \neq 0$, 那么有如下论断 (见表 8.11).

表 8.11 A 的型及相应的情况

A 的型	添加列满足的条件	A 的个数
$2i+3$	$V_{11}, V_{12}, V_{21}, V_{22}, a', b'$ 任意, $V_{31} = V_{32} = 0$, $w_2 = 0, w_1 \neq 0, c' + w_1^{-2}b'^2 \neq 0$	$q^{4i+2}(q-1)^2$
$2i+3$	$V_{11}, V_{12}, V_{21}, V_{22}, w_1, b', c'$ 任意, $V_{31} = V_{32} = 0$, $w_2 \neq 0, a' \neq w_2^{-1}w_1b' + w_2^{-2}w_1^2c' + w_2^{-2}b'^2$	$q^{4i+3}(q-1)^2$
$2(i+1)^+$	$V_{11}, V_{12}, V_{21}, V_{22}, b'$ 任意, $V_{31} = V_{32} = 0$, $w_2 = 0, w_1 \neq 0,\ c' + w_1^{-2}b'^2 = 0,\ a' \in w_1^2N$	$\frac{1}{2}q^{4i+2}(q-1)$
$2(i+1)^+$	$V_{11}, V_{12}, V_{21}, V_{22}, w_1, b'$ 任意, $V_{31} = V_{32} = 0$, $w_2 \neq 0, c' \in w_2^2N$ $a' = w_2^{-1}w_1b' + w_2^{-2}w_1^2c' + w_2^{-2}b'^2$	$\frac{1}{2}q^{4i+3}(q-1)$
$2(i+1)^-$	$V_{11}, V_{12}, V_{21}, V_{22}, b'$ 任意, $V_{31} = V_{32} = 0, w_2 = 0$, $w_1 \neq 0, c' + w_1^{-2}b'^2 = 0, a' \notin w_1^2N$	$\frac{1}{2}q^{4i+2}(q-1)$
$2(i+1)^-$	$V_{11}, V_{12}, V_{21}, V_{22},\ w_1, b'$ 任意, $V_{31} = V_{32} = 0$, $w_2 \neq 0, c' \notin w_2^2N$ $a' = w_2^{-1}w_1b' + w_2^{-2}w_1^2c' + w_2^{-2}b'^2$	$\frac{1}{2}q^{4i+3}(q-1)$

(IIIb) 设 $\mathrm{rank}(V_{31}V_{32}) = 1\,(n-2i-3 \geqslant 1)$. 这时

$$A \sim \left(\begin{array}{ccccc|cc} 0 & I^{(i)} & & & & 0 & 0 \\ & 0 & & & & 0 & 0 \\ & & 1 & & & w_1 & w_2 \\ & & & 0^{n-2i-4} & & 0 & 0 \\ & & & & 0 & u & v \\ \hline & & & & & a' & b' \\ & & & & & & c' \end{array}\right),$$

(IIIb1) 如果 $\text{rank}\begin{pmatrix} w_1 & w_2 \\ u & v \end{pmatrix} = 1$, 即 $(w_1, w_2) = \lambda(u, v)$, 那么有如下论断 (见表 8.12).

表 8.12 A 的型及相应的情况

A 的型	添加列满足的条件	A 的个数
$2i+3$	$V_{11}, V_{12}, V_{21}, V_{22}, a', b', c'$ 任意, $\text{rank}(V_{31}\ V_{32}) = 1, (w_1, w_2) = \lambda(u, v), v = 0, u \neq 0$	$q^{4i+4}(q^{n-2i-3}-1)$
$2i+3$	$V_{11}, V_{12}, V_{21}, V_{22}, u, a', b', c'$ 任意, $\text{rank}(V_{31}\ V_{32}) = 1, (w_1, w_2) = \lambda(u, v), v \neq 0$	$q^{4i+5}(q^{n-2i-3}-1)$

(IIIb2) 如果 $\text{rank}\begin{pmatrix} w_1 & w_2 \\ u & v \end{pmatrix} = 2$, 那么有如下论断 (见表 8.13).

表 8.13 A 的型及相应的情况

A 的型	添加列满足的条件	A 的个数
$2(i+2)^+$	$V_{11}, V_{12}, V_{21}, V_{22}, w_1, a', b'$ 任意, $w_1 v + w_2 u \neq 0, v = 0, u \neq 0, w_2 \neq 0, c' \in w_2^2 N$	$\frac{1}{2}q^{4i+4}(q^{n-2i-3}-1)(q-1)$
$2(i+2)^+$	$V_{11}, V_{12}, V_{21}, V_{22}, u, w_2, b', c'$ 任意, $w_1 v + w_2 u \neq 0, v \neq 0, w_1' = w_1 - v^{-1}uw_2 \neq 0, a' + v^{-2}u^2 c' + v^{-1}u b' \in {w_1'}^2 N$	$\frac{1}{2}q^{4i+5}(q^{n-2i-3}-1)(q-1)$
$2(i+2)^-$	$V_{11}, V_{12}, V_{21}, V_{22}, w_1, a', b'$ 任意, $w_1 v + w_2 u \neq 0, v = 0, u \neq 0, w_2 \neq 0, c' \notin w_2^2 N$	$\frac{1}{2}q^{4i+4}(q^{n-2i-3}-1)(q-1)$
$2(i+2)^-$	$V_{11}, V_{12}, V_{21}, V_{22}, u, w_2, b', c'$ 任意, $w_1 v + w_2 u \neq 0, v \neq 0, w_1' = w_1 - v^{-1}uw_2 \neq 0, a' + v^{-2}u^2 c' + v^{-1}u b' \notin {w_1'}^2 N$	$\frac{1}{2}q^{4i+5}(q^{n-2i-3}-1)(q-1)$

(IIIc) 设 $\text{rank}(V_{31}V_{32}) = 2$ $(n-2i-3 \geqslant 2)$. 这时

$$A \sim \left[\begin{pmatrix} 0 & I^{(i)} \\ & 0 \end{pmatrix}, 1, 0^{(n-2i-5)}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ & 0 & 0 & 1 \\ & & a' & b' \\ & & & c' \end{pmatrix}\right].$$

我们有如下论断 (见表 8.14).

表 8.14 A 的型及相应的情况

A 的型	添加列满足的条件	A 的个数
$2i+5$	$V_{11}, V_{12}, V_{21}, V_{22}, w_1, w_2, a', b', c'$ 任意, $\text{rank}(V_{31}\ V_{32}) = 2,$	$q^{4i+6}(q^{n-2i-3}-1)(q^{n-2i-4}-1)$

根据上面对二次型的 2 扩充的论断, 我们有

定理 8.14　对于各类二次型个数, 我们有如下计数公式:

(i) $|C_{2i^+}^{(n)}| = q^{4i}|C_{2i^+}^{(n-2)}| + \frac{1}{2}q^{4i-2}(q^2-1)|C_{2i-1}^{(n-2)}| + \big(\frac{1}{2}q^{4i-3}(q^2-1)$

$\quad + q^{4i-2}(q+1)(q^{n-2i}-1)\big)|C_{2(i-1)^+}^{(n-2)}| + \frac{1}{2}q^{4i-3}(q-1)^2|C_{2(i-1)^-}^{(n-2)}|$

$\quad + \frac{1}{2}q^{4i-4}(q^2-1)(q^{n-2i+1}-1)|C_{2i-3}^{(n-2)}|$

$\quad + q^{4i-4}(q^{n-2i+2}-1)(q^{n-2i+1}-1)|C_{2(i-2)^+}^{(n-2)}|.$

(ii) $|C_{2i^-}^{(n)}| = q^{4i}|C_{2i^-}^{(n-2)}| + \frac{1}{2}q^{4i-2}(q^2-1)|C_{2i-1}^{(n-2)}| + \frac{1}{2}q^{4i-3}(q-1)^2|C_{2(i-1)^+}^{(n-2)}|$

$\quad + \big(\frac{1}{2}q^{4i-3}(q^2-1) + q^{4i-2}(q+1)(q^{n-2i}-1)\big)|C_{2(i-1)^-}^{(n-2)}|$

$\quad + \frac{1}{2}q^{4i-4}(q^2-1)(q^{n-2i+1}-1)|C_{2i-3}^{(n-2)}|$

$\quad + q^{4i-4}(q^{n-2i+2}-1)(q^{n-2i+1}-1)|C_{2(i-2)^-}^{(n-2)}|.$

(iii) $|C_{2i+1}^{(n)}| = q^{4i+2}|C_{2i+1}^{(n-2)}| + q^{4i}(q^2-1)\left(|C_{2i^+}^{(n-2)}| + |C_{2i^-}^{(n-2)}|\right)$

$\quad + q^{4i}(q^{n-2i}+q^{n-2i-1}-2)|C_{2i-1}^{(n-2)}|$

$\quad + q^{4i-2}(q^2-1)(q^{n-2i}-1)\left(|C_{2(i-1)^+}^{(n-2)}| + |C_{2(i-1)^-}^{(n-2)}|\right)$

$\quad + q^{4i-2}(q^{n-2i}-1)(q^{n-2i+1}-1)|C_{2i-3}^{(n-2)}|.$

证明　根据上面的讨论分析各类二次型的构成即得.　□

定理 8.14 中的三个公式可以两次应用定理 8.7 中的公式导出来, 这三个公式之所以需要, 是因为秩为 $2k$ 的交错矩阵对应特征标 $f_{2k^*}^{(n)}$ 在递归计算时要归结到 $f_{2(k-1)^*}^{(n-2)}$, $f_{2(k-2)^*}^{(n-4)}$ 等等. 从阶数上说是 2− 递减的. 因此在应用上面的三个公式时 n 必须是偶数 (见定理 8.15 和 8.16).

平行于定理 8.8 和 8.9 我们有

定理 8.15　设 $n = 2m$, 且 $k < m$. 那么秩为 $2k$ 的交错矩阵对应特征标满足下面的等式:

(i) $f_{2k^*}^{(2m)}(C_{2i^+}^{(2m)})$

$= q^{4i}f_{2k^*}^{(2m-2)}(C_{2i^+}^{(2m-2)}) + \frac{1}{2}q^{4i-2}(q^2-1)f_{2k^*}^{(2m-2)}(C_{2i-1}^{(2m-2)})$

$\quad + \big(\frac{1}{2}q^{4i-3}(q^2-1) + q^{4i-2}(q+1)(q^{2m-2i}-1)\big)f_{2k^*}^{(2m-2)}(C_{2(i-1)^+}^{(2m-2)})$

$\quad + \frac{1}{2}q^{4i-3}(q-1)^2 f_{2k^*}^{(2m-2)}(C_{2(i-1)^-}^{(2m-2)})$

$\quad + \frac{1}{2}q^{4i-4}(q^2-1)(q^{2m-2i+1}-1)f_{2k^*}^{(2m-2)}(C_{2i-3}^{(2m-2)})$

$\quad + q^{4i-4}(q^{2m-2i+2}-1)(q^{2m-2i+1}-1)f_{2k^*}^{(2m-2)}(C_{2(i-2)^+}^{(2m-2)}).$

(ii) $f_{2k^*}^{(2m)}(C_{2i^-}^{(2m)})$

$$\begin{aligned}&= q^{4i}f_{2k^*}^{(2m-2)}(C_{2i^-}^{(2m-2)}) + \tfrac{1}{2}q^{4i-2}(q^2-1)f_{2k^*}^{(2m-2)}(C_{2i-1}^{(2m-2)})\\ &\quad + \tfrac{1}{2}q^{4i-3}(q-1)^2f_{2k^*}^{(2m-2)}(C_{2(i-1)^+}^{(2m-2)})\\ &\quad + \left(\tfrac{1}{2}q^{4i-3}(q^2-1)+q^{4i-2}(q+1)(q^{2m-2i}-1)\right)f_{2k^*}^{(2m-2)}(C_{2(i-1)^-}^{(2m-2)})\\ &\quad + \tfrac{1}{2}q^{4i-4}(q^2-1)(q^{2m-2i+1}-1)f_{2k^*}^{(2m-2)}(C_{2i-3}^{(2m-2)})\\ &\quad + q^{4i-4}(q^{2m-2i+2}-1)(q^{2m-2i+1}-1)f_{2k^*}^{(2m-2)}(C_{2(i-2)^-}^{(2m-2)}).\end{aligned}$$

(iii) $f_{2k^*}^{(2m)}(C_{2i+1}^{(2m)})$

$$\begin{aligned}&= q^{4i+2}f_{2k^*}^{(2m-2)}(C_{2i+1}^{(2m-2)})\\ &\quad + q^{4i}(q^{2m-2i}+q^{2m-2i-1}-2)f_{2k^*}^{(2m-2)}(C_{2i-1}^{(2m-2)})\\ &\quad + q^{4i}(q^2-1)\left(f_{2k^*}^{(2m-2)}(C_{2i^+}^{(2m-2)})+f_{2k^*}^{(2m-2)}(C_{2i^-}^{(2m-2)})\right)\\ &\quad + q^{4i-2}(q^2-1)(q^{2m-2i}-1)\left(f_{2k^*}^{(2m-2)}(C_{2(i-1)^+}^{(2m-2)})+f_{2k^*}^{(2m-2)}(C_{2(i-1)^-}^{(2m-2)})\right)\\ &\quad + q^{4i-2}(q^{2m-2i}-1)(q^{2m-2i+1}-1)f_{2k^*}^{(2m-2)}(C_{2i-3}^{(2m-2)}).\end{aligned}$$

证明　由定理 8.14 立得. □

定理 8.16　设 $n=2m$, 那么秩为 $2m$ 的交错矩阵对应特征标 $f_{2m^*}^{(2m)}$ 满足下面的等式:

(i) $$f_{2m^*}^{(2m)}(C_{2i^+}^{(2m)}) = q^{2i}f_{2(m-1)^*}^{(2m-2)}(C_{2i^+}^{(2m-2)}) - \tfrac{1}{2}q^{2i-1}(q+1)f_{2(m-1)^*}^{(2m-2)}(C_{2(i-1)^+}^{(2m-2)}) - \tfrac{1}{2}q^{2i-1}(q-1)f_{2(m-1)^*}^{(2m-2)}(C_{2(i-1)^-}^{(2m-2)}).$$

(ii) $$f_{2m^*}^{(2m)}(C_{2i^-}^{(2m)}) = q^{2i}f_{2(m-1)^*}^{(2m-2)}(C_{2i^-}^{(2m-2)}) - \tfrac{1}{2}q^{2i-1}(q-1)f_{2(m-1)^*}^{(2m-2)}(C_{2(i-1)^+}^{(2m-2)}) - \tfrac{1}{2}q^{2i-1}(q+1)f_{2(m-1)^*}^{(2m-2)}(C_{2(i-1)^-}^{(2m-2)}).$$

(iii) $$f_{2m^*}^{(2m)}(C_{2i+1}^{(2m)}) = q^{2i}(q^2-1)\left(f_{2(m-1)^*}^{(2m-2)}(C_{2i^+}^{(2m-2)})+f_{2(m-1)^*}^{(2m-2)}(C_{2i^-}^{(2m-2)})\right) + q^{2i+2}f_{2(m-1)^*}^{(2m-2)}(C_{2i+1}^{(2m-2)}) - q^{2i}f_{2(m-1)^*}^{(2m-2)}(C_{2i-1}^{(2m-2)}).$$

证明　(i) 仿定理 8.7 的证明, 根据上面关于 $2m-2$ 元二次型的 2 扩充的论断, 考虑 $C_{2i^+}^{(2m)}$ 由 $2m-2$ 元二次型的那些 2 扩充组成. 然后考虑这些 2 扩充对于 $f_{2m^*}^{(2m)}(C_{2i^+}^{(2m)})$ 的贡献, 它们中只有三部分是有贡献的, 即

$$\begin{aligned}f_{2m^*}^{(2m)}(C_{2i^+}^{(2m)}) =& f_{2(m-1)^*}^{(2m-2)}(C_{2i^+}^{(2m-2)})\cdot \sum_{\substack{v_{11},v_{12},v_{21},v_{22}\\ \text{任意},\, b'={}^tv_{11}v_{22}+{}^tv_{12}v_{21}}} \chi(b')\\ &+ f_{2(m-1)^*}^{(2m-2)}(C_{2(i-1)^+}^{(2m-2)})\cdot \sum_{\substack{v_{11},v_{12},v_{21},v_{22}\text{任意}\\ b'=b+{}^tv_{11}v_{22}+{}^tv_{12}v_{21}\neq 0,\ a'c'\in b'^2N}} \chi(b')\end{aligned}$$

$$+ f^{(2m-2)}_{2(m-1)^*}(C^{(2m-2)}_{2(i-1)^-}) \cdot \sum_{\substack{V_{11}, V_{12}, V_{21}, V_{22}, w_{11}, w_{12}, w_{21}, w_{22}\text{任意} \\ b'=b+{}^tV_{11}V_{22}+{}^tV_{12}V_{22} \\ +w_{11}w_{22}+w_{12}w_{22}\neq 0,\ a'c'\notin b'^2N}} \chi(b')$$

由引理 8.1~ 引理 8.5, 可知 (i) 式成立.

类似地可以证明 (ii) 和 (iii) 都成立. □

定理 8.17 我们恒有 $f^{(n)}_{2k^*}(C^{(n)}_1) = q^n - 1$, $k = 1, 2, \cdots, [\frac{n}{2}]$.

证明 由定义有

$$f^{(n)}_{2k^*}\left(\left\{\left(\begin{matrix} x_1 & & \\ & \cdots & \\ & & x_n \end{matrix}\right) \middle| (x_1, \cdots, x_n) \neq 0\right\}\right) = \sum_{(x_1,\cdots,x_n)\neq 0} \overbrace{\chi(0)\cdots\chi(0)}^{k}$$
$$= q^n - 1.$$
□

应用定理 8.15~ 定理 8.17 中提供的公式, 我们就可以计算 $f^{(n)}_{2k^*}$ 在各类二次型集合上之值. 但应注意, 如果 n 为奇数 (这时自然有 $2k < n$), 需先应用定理 8.7 中提供的公式, 将 $|C^{(n)}_{2i^+}|$, $|C^{(n)}_{2i^-}|$ 和 $|C^{(n)}_{2i+1}|$ 写成相应的各类 $n-1$ 元二次型个数的组合, 然后再应用定理 8.15~ 定理 8.17. §8.8 中 $n = 3, 4$ 情形中 $f^{(n)}_{2k^*}$ 之值就是这样计算出来的.

§8.6 $f^{(n)}_{2k^*}$ 在合并类 $C^{(n)}_{2i}$ 和 $C^{(n)}_{2i} \cup C^{(n)}_{2i-1}$ 上的取值

首先, 由定理 8.15 和 8.16 可得

定理 8.18 对于 $f^{(n)}_{2k^*}$ 在合并类 $C^{(n)}_{2i}$ 上的取值, 我们有如下公式:

(i) 对于 $k < m$, 我们有

$$\begin{aligned} f^{(2m)}_{2k^*}(C^{(2m)}_{2i}) = & q^{4i} f^{(2m-2)}_{2k^*}(C^{(2m-2)}_{2i}) + q^{4i-2}(q^2-1) f^{(2m-2)}_{2k^*}(C^{(2m-2)}_{2i-1}) \\ & + q^{4i-2}(q^{2m-2i+1} + q^{2m-2i} - 2) f^{(2m-2)}_{2k^*}(C^{(2m-2)}_{2i-2}) \\ & + q^{4i-4}(q^2-1)(q^{2m-2i+1}-1) f^{(2m-2)}_{2k^*}(C^{(2m-2)}_{2i-3}) \\ & + q^{4i-4}(q^{2m-2i+1}-1)(q^{2m-2i+2}-1) f^{(2m-2)}_{2k^*}(C^{(2m-2)}_{2i-4}). \end{aligned}$$

(ii) $f^{(2m)}_{2m^*}(C^{(2m)}_{2i}) = q^{2i} f^{(2m-2)}_{2(m-1)^*}(C^{(2m-2)}_{2i}) - q^{2i} f^{(2m-2)}_{2(m-1)^*}(C^{(2m-2)}_{2i-2})$.

(iii) 特别地, $f^{(2m)}_{2m^*}(C^{(2m)}_{2m}) = (-1)^m q^{m(m+1)}$.

其次, 我们可以将 $f^{(2m)}_{2k^*}$ 和 $f^{(2m)}_{2m^*}$ 在秩为 $2i-1$ 的类 $C^{(2m)}_{2i-1}$ 上取值公式改写成下面的

定理 8.19 对于 $f^{(2m)}_{2k^*}$ 和 $f^{(2m)}_{2m^*}$ 在类 $C^{(2m)}_{2i-1}$ 上取值, 我们有

(i) 设 $k < m$. 那么

$$\begin{aligned}f_{2k^*}^{(2m)}(C_{2i-1}^{(2m)})=&q^{4i-2}f_{2k^*}^{(2m-2)}(C_{2i-1}^{(2m-2)})+q^{4i-4}(q^2-1)f_{2k^*}^{(2m-2)}(C_{2i-2}^{(2m-2)})\\&+q^{4i-4}(q^{2m-2i+2}+q^{2m-2i+1}-2)f_{2k^*}^{(2m-2)}(C_{2i-3}^{(2m-2)})\\&+q^{4i-6}(q^2-1)(q^{2m-2i+2}-1)f_{2k^*}^{(2m-2)}(C_{2i-4}^{(2m-2)})\\&+q^{4i-6}(q^{2m-2i+2}-1)(q^{2m-2i+3}-1)f_{2k^*}^{(2m-2)}(C_{2i-5}^{(2m-2)}).\end{aligned}$$

(ii) $$\begin{aligned}f_{2m^*}^{(2m)}(C_{2i-1}^{(2m)})=&q^{2i}f_{2(m-1)^*}^{(2m-2)}(C_{2i-1}^{(2m-2)})+q^{2i-2}(q^2-1)f_{2(m-1)^*}^{(2m-2)}(C_{2i-2}^{(2m-2)})\\&-q^{2i-2}f_{2(m-1)^*}^{(2m-2)}(C_{2i-3}^{(2m-2)}).\end{aligned}$$

现在, 我们来证明下面的重要定理

定理 8.20 对于任何 n, 我们有

$$f_{2k^*}^{(n)}(C_{2i}^{(n)}\cup C_{2i-1}^{(n)})=f_{2k}^{(n)}(C_{2i}^{(n)}\cup C_{2i-1}^{(n)}).$$

证明 对 n 用归纳法. 由 §8.8 知, $n=2, 3, 4$ 时这个论断成立. 现在设 $n\geqslant 5$, 并且假设对于 $<n$ 的情形本论断成立. 往证对于 n 的情形, 本论断亦成立.

如果 n 为奇数, 那么 $2k<2n$, 这时由定理 8.8(iii), 定理 8.12(i) 和定理 8.11, 有

$$\begin{aligned}f_{2k}^{(n)}(C_{2i}^{(n)})&=q^{2i}f_{2k}^{(n-1)}(C_{2i}^{(n-1)})+(q^n-q^{2i})f_{2k}^{(n-1)}(C_{2i-2}^{(n-1)})\\&=q^{2i}f_{2k}^{(n-1)}(C_{2i}^{(n-1)}\cup(C_{2i-1}^{(n-1)})+q^nf_{2k}^{(n-1)}(C_{2i-2}^{(n-1)}).\end{aligned}$$

$$\begin{aligned}f_{2k}^{(n)}(C_{2i-1}^{(n)})&=q^{2i-1}f_{2k}^{(n-1)}(C_{2i-1}^{(n-1)})+q^{2i-2}(q-1)f_{2k}^{(n-1)}(C_{2i-2}^{(n-1)})\\&\quad+q^{2i-2}(q^{n-2i+2}-1)f_{2k}^{(n-1)}(C_{2i-3}^{(n-1)})\\&=-q^{2i-2}f_{2k}^{(n-1)}(C_{2i-2}^{(n-1)})+q^{2i-2}(q^{n-2i+2}-1)f_{2k}^{(n-1)}(C_{2i-3}^{(n-1)}).\end{aligned}$$

于是

$$\begin{aligned}f_{2k}^{(n)}(C_{2i}^{(n)}\cup C_{2i-1}^{(n)})=&q^{2i}f_{2k}^{(n-1)}(C_{2i}^{(n-1)}\cup C_{2i-1}^{(n-1)})\\&+(q^n-q^{2i-2})f_{2k}^{(n-1)}(C_{2i-2}^{(n-1)}\cup C_{2i-3}^{(n-1)}).\end{aligned}\tag{8.4}$$

另一方面, 由于 $2k<n$, 由定理 8.7(i), (ii), (iii), 仿定理 8.8 的证明可知有

$$\begin{aligned}f_{2k^*}^{(n)}(C_{2i}^{(n)})=&q^{2i}f_{2k^*}^{(n-1)}(C_{2i}^{(n-1)})+(q^{2i}-q^{2i-1})f_{2k^*}^{(n-1)}(C_{2i-1}^{(n-1)})\\&+(q^n-q^{2i-1})f_{2k^*}^{(n-1)}(C_{2i-2}^{(n-1)}),\end{aligned}$$

$$\begin{aligned}f_{2k^*}^{(n)}(C_{2i-1}^{(n)})=&q^{2i-1}f_{2k^*}^{(n-1)}(C_{2i-1}^{(n-1)})+(q^{2i-1}-q^{2i-2})f_{2k^*}^{(n-1)}(C_{2i-2}^{(n-1)})\\&+(q^n-q^{2i-2})f_{2k^*}^{(n-1)}(C_{2i-3}^{(n-1)}).\end{aligned}$$

于是

$$\begin{aligned}f_{2k^*}^{(n)}(C_{2i}^{(n)}\cup C_{2i-1}^{(n)})=&q^{2i}f_{2k^*}^{(n-1)}(C_{2i}^{(n-1)}\cup C_{2i-1}^{(n-1)})\\&+(q^n-q^{2i-2})f_{2k^*}^{(n-1)}(C_{2i-2}^{(n-1)}\cup C_{2i-3}^{(n-1)}).\end{aligned}\tag{8.5}$$

由 (8.4) 和 (8.5) 式, 立知只需考虑 n 为偶数的情形就可以了.

下面设 $n=2m$. 往证本论断亦成立.

当 $k<m$ 时, 由定理 8.18(i), 8.19(i), 有

$$\begin{aligned}f_{2k^*}^{(2m)}(C_{2i}^{(2m)}) =& q^{4i}f_{2k^*}^{(2m-2)}(C_{2i}^{(2m-2)}) + (q^{4i}-q^{4i-2})f_{2k^*}^{(2m-2)}(C_{2i-1}^{(2m-2)})\\ &+ q^{4i-2}(q^{2m-2i+1}+q^{2m-2i}-2)f_{2k^*}^{(2m-2)}(C_{2i-2}^{(2m-2)})\\ &+ q^{4i-4}(q^2-1)(q^{2m-2i+1}-1)f_{2k^*}^{(2m-2)}(C_{2i-3}^{(2m-2)})\\ &+ q^{4i-4}(q^{2m-2i+1}-1)(q^{2m-2i+2}-1)f_{2k^*}^{(2m-2)}(C_{2i-4}^{(2m-2)}).\end{aligned}$$

$$\begin{aligned}f_{2k^*}^{(2m)}(C_{2i-1}^{(2m)}) =& q^{4i-2}f_{2k^*}^{(2m-2)}(C_{2i-1}^{(2m-2)}) + (q^{4i-2}-q^{4i-4})f_{2k^*}^{(2m-2)}(C_{2i-2}^{(2m-2)})\\ &+ q^{4i-4}(q^{2m-2i+2}+q^{2m-2i+1}-2)f_{2k^*}^{(2m-2)}(C_{2i-3}^{(2m-2)})\\ &+ q^{4i-6}(q^2-1)(q^{2m-2i+2}-1)f_{2k^*}^{(2m-2)}(C_{2i-4}^{(2m-2)})\\ &+ q^{4i-6}(q^{2m-2i+2}-1)(q^{2m-2i+3}-1)f_{2k^*}^{(2m-2)}(C_{2i-5}^{(2m-2)}).\end{aligned}$$

于是有

$$\begin{aligned}&f_{2k^*}^{(2m)}(C_{2i}^{(2m)}\cup C_{2i-1}^{(2m)})\\ =&q^{4i}f_{2k^*}^{(2m-2)}(C_{2i}^{(2m-2)}\cup C_{2i-1}^{(2m-2)})\\ &+(q^{2m+2i-1}+q^{2m+2i-2}-q^{4i-2}-q^{4i-4})f_{2k^*}^{(2m-2)}(C_{2i-2}^{(2m-2)}\cup C_{2i-3}^{(2m-2)})\\ &+q^{4i-6}(q^{2m-2i+2}-1)(q^{2m-2i+3}-1)f_{2k^*}^{(2m-2)}(C_{2i-4}^{(2m-2)}\cup C_{2i-5}^{(2m-2)}).\end{aligned}$$

另一方面, 由于 $2k<2m$, 我们两次应用定理 8.20 的证明中之 (8.4) 式可得

$$\begin{aligned}&f_{2k}^{(2m)}(C_{2i}^{(2m)}\cup C_{2i-1}^{(2m)})\\ =&q^{4i}f_{2k}^{(2m-2)}(C_{2i}^{(2m-2)})\cup C_{2i-1}^{(2m-2)})\\ &+(q^{2m+2i-1}+q^{2m+2i-2}-q^{4i-2}-q^{4i-4})f_{2k}^{(2m-2)}(C_{2i-2}^{(2m-2)}\cup C_{2i-3}^{(2m-2)})\\ &+q^{4i-6}(q^{2m-2i+2}-1)(q^{2m-2i+3}-1)f_{2k}^{(2m-2)}(C_{2i-4}^{(2m-2)}\cup C_{2i-5}^{(2m-2)}).\end{aligned}$$

比较上面两式的对应项, 由归纳假设可知两式右端相等, 因而左端相等.

剩下来考虑 $k=m$ 的情形, 由定理 8.18(ii) 和定理 8.19(ii), 有

$$\begin{aligned}f_{2m^*}^{(2m)}(C_{2i}^{(2m)}\cup C_{2i-1}^{(2m)}) =& q^{2i}f_{2(m-1)^*}^{(2m-2)}(C_{2i}^{(2m-2)}\cup C_{2i-1}^{(2m-2)})\\ &-q^{2i-2}f_{2(m-1)^*}^{(2m-2)}(C_{2i-2}^{(2m-2)}\cup C_{2i-3}^{(2m-2)}).\end{aligned}\tag{8.6}$$

另一方面, 由定理 8.12(ii) 和定理 8.11, 有

$$\begin{aligned}f_{2m}^{(2m)}(C_{2i}^{(2m)}) &= q^{2i}f_{2m-2}^{(2m-2)}(C_{2i}^{(2m-2)}) - q^{2i}f_{2m-2}^{(2m-2)}(C_{2i-2}^{(2m-2)})\\ &= q^{2i}f_{2m-2}^{(2m-2)}(C_{2i}^{(2m-2)}\cup C_{2i-1}^{(2m-2)}).\end{aligned}$$

再由定理 8.11 和上式有

$$\begin{aligned}f_{2m}^{(2m)}(C_{2i-1}^{(2m)}) &= -f_{2m}^{(2m)}(C_{2i-2}^{(2m)})\\ &= -q^{2i-2}f_{2m-2}^{(2m-2)}(C_{2i-2}^{(2m-2)}\cup C_{2i-3}^{(2m-2)}).\end{aligned}$$

于是得

$$\begin{aligned}f_{2m}^{(2m)}(C_{2i}^{(2m)}\cup C_{2i-1}^{(2m)}) = &\, q^{2i}f_{2m-2}^{(2m-2)}(C_{2i}^{(2m-2)}\cup C_{2i-1}^{(2m-2)})\\ &- q^{2i-2}f_{2m-2}^{(2m-2)}(C_{2i-2}^{(2m-2)}\cup C_{2i-3}^{(2m-2)}).\end{aligned} \tag{8.7}$$

由归纳假设 (8.6), (8.7) 两式右端相等, 因而它们的左端相等. 本定理得证. □

由定理 8.13 和定理 8.20. 立得

定理 8.21 对任何整数 $n \geqslant 2$, 都有

$$\begin{aligned}f_{2k^*}^{(n)}(C_{2i}^{(n)}\cup C_{2i-1}^{(n)}) &= f_{2k}^{(n)}(C_{2i}^{(n)}\cup C_{2i-1}^{(n)})\\ &= f_{2k-1}^{(n)}(C_{2i}^{(n)}\cup C_{2i-1}^{(n)}),\ k, i = 1, 2, \cdots, \left[\frac{n}{2}\right].\end{aligned}$$

§8.7 $\widetilde{\mathrm{Q}}\mathrm{ua}\,(n,\,q)$ 的对偶方案

设 $\mathbb{F}_q$ 为特征数为 2 的有限域, $n \geqslant 2$. 由定理 7.15 知, $\mathbb{F}_q$ 上的 n 元二次型结合方案 $\mathrm{Qua}(n, q)$ 和 $\mathbb{F}_q$ 上的 $n\times n$ 对称矩阵结合方案 $\mathrm{Sym}(n, q)$ 是形式对偶的. 在这一节中, 我们利用本章中得到的关于 $\mathrm{Qua}(n, q)$ 的特征值的性质来讨论 $\mathrm{Qua}(n, q)$ 的聚合方案 $\widetilde{\mathrm{Q}}\mathrm{ua}(n, q)$ 在 $\mathrm{Sym}(n, q)$ 中导出的对偶方案.

回忆在 §8.1 中, 我们用 D_r 表示 $S(n, q)$ 中秩为 r 的非交错对称矩阵的合同类, $r = 0, 1, \cdots, n$; 用 D_{2s^*} 表示 $S(n, q)$ 中秩为 $2s$ 的交错对称矩阵的合同类, $s = 1, \cdots, [\frac{n}{2}]$. 再令 $\widetilde{D}_{2k-1} = D_{2k-1}\cup D_{2k}$, 如果 n 为奇数, 则令 $\widetilde{D}_n = D_n$; 令 $\widetilde{D}_{2k} = D_{2k^*}$, $k = 1, \cdots, [\frac{n}{2}]$; 再令 $\widetilde{D}_0 = D_0$,

$$W_i = \{(S_1, S_2)|S_2 - S_1 \in \widetilde{D}_i\},\ i = 0, 1, \cdots, n.$$

我们有下面的

定理 8.22 设 $\mathbb{F}_q$ 为特征数为 2 的 q 元域, $n \geqslant 2$. 那么 $\mathfrak{Y} = (S(n, q), \{W_i\}_{0\leqslant i\leqslant n})$ 是一个结合方案, 记作 $\widetilde{\mathrm{S}}\mathrm{ym}\,(n, q)$, 它与结合方案 $\widetilde{\mathrm{Q}}\mathrm{ua}(n, q)$ 是形式对偶的.

证明 如 (8.1) 中所定义, 映射 $A \longmapsto f_A$ 将 $S(n, q)$ 和 $Q(n, q)$ 的特征标群 $Q(n, q)^*$ 等同起来. 由定理 7.21 知, $\mathrm{Qua}(n, q)$ 的聚合方案 $\widetilde{\mathrm{Q}}\mathrm{ua}(n, q) = (Q(n, q), \{R_i\}_{0\leqslant i\leqslant n})$, 这里

$$R_{2s} = R_{2s^+}\cup R_{2s^-},\ R_{2s+1} = R_{2s+1},\ s = 0, 1, \cdots, \left[\frac{n}{2}\right].$$

记 $C_{2s} = C_{2s+}^{(n)} \cup C_{2s-}^{(n)}$, $C_{2s+1} = C_{2s+1}^{(n)}$, 于是 $R_i = \{(X, Y)|Y - X \in C_i\}$, $i = 0, 1, \cdots, n$. $C_0, C_1, \cdots, C_n$ 作成 $\mathrm{Qua}(n, q)$ 的一个分划. 由于 $\widetilde{\mathrm{Qua}}(n, q)$ 是结合方案, 这个分划导出加法群 $Q(n, q)$ 上的一个 S 环 $\mathfrak{S}$, 而 $\mathfrak{S}$ 决定的结合方案就是 $\widetilde{\mathrm{Qua}}(n, q)$. 定理 8.13 给出

$$f_{2k-1}(C_j) = f_{2k}(C_j), \ j = 0, 1, \cdots, n.$$

所以特征标 f_{2k-1} 和 f_{2k} 在 $\mathfrak{S}$ 上取值相同, 于是由定理 1.14(S 环的对偶性), f_{2k-1} 和 f_{2k} 在特征标群 $S(n, q)$ 中确定的同一等价类中. 由于 f_{2k-1} 和 f_{2k} 分别是由 D_{2k-1} 和 D_{2k} 中的对称矩阵确定的特征标, 所以 $S(n, q)$ 中确定的等价类恰为由 $\widetilde{D}_i$ 所确定的那些等价类 ($i = 0, 1, \cdots, n$). 这些等价类给出的 $S(n, q)$ 上的结合方案就是 $\mathcal{Y}$, 因而它与 $\widetilde{\mathrm{Qua}}(n, q)$ 是形式对偶的. □

现在我们将 $\widetilde{\mathrm{Qua}}(n, q)$ 的结合类再行合并, 令

$$\overline{R}_i = R_{2i} \cup R_{2i-1}, \quad i = 1, 2, \cdots, \left[\frac{n+1}{2}\right],$$

再令 $\overline{R}_0 = R_0$. 那么结合方案 $\mathrm{Quad}\ (n, q) = (Q(n, q), \{\overline{R}_i\}_{0 \leqslant i \leqslant [\frac{n+1}{2}]})$, 由定理 8.21. 仿上讨论, 立得

定理 8.23　设 $\mathbb{F}_q$ 为特征数为 2 的有限域, $n \geqslant 2$. 那么 $\mathbb{F}_q$ 上的结合方案 $\mathrm{Quad}(n, q)$ 与 $\mathbb{F}_q$ 上的对称矩阵结合方案 $\mathrm{Sym}(n, q)$ 的聚合方案 $\overline{\mathrm{Sym}}(n, q)$ 是形式对偶的.

§8.8　二次型方案的特征值 (特征数 = 2)

最后, 我们列表分别给出 $n = 2, 3, 4$ 时二次型结合方案的特征值 (见表 8.15～表 8.23).

1. $n = 2$.

表 8.15　Qua(2, q) 的特征值

	$C_0^{(2)}$	$C_1^{(2)}$	$C_{2+}^{(2)}$	$C_{2-}^{(2)}$
$f_0^{(2)}$	1	q^2-1	$\frac{1}{2}q(q^2-1)$	$\frac{1}{2}q(q-1)^2$
$f_1^{(2)}$	1	-1	$\frac{1}{2}q(q-1)$	$-\frac{1}{2}q(q-1)$
$f_2^{(2)}$	1	-1	$-\frac{1}{2}q$	$\frac{1}{2}q$
$f_{2^*}^{(2)}$	1	q^2-1	$-\frac{1}{2}q(q+1)$	$-\frac{1}{2}q(q-1)$

表 8.16 $\widetilde{\text{Qua}}(2,\ q)$ 的特征值

	$C_0^{(2)}$	$C_1^{(2)}$	$C_2^{(2)}$
$f_0^{(2)}$	1	q^2-1	$q^2(q-1)$
$f_1^{(2)},\ f_2^{(2)}$	1	-1	0
$f_{2^*}^{(2)}$	1	q^2-1	$-q^2$

第一特征值矩阵

$$P=\begin{pmatrix} 1 & q^2-1 & q^2(q-1) \\ 1 & -1 & 0 \\ 1 & q^2-1 & -q^2 \end{pmatrix}.$$

第二特征值矩阵

$$Q=q^3P^{-1}=\begin{pmatrix} 1 & q(q^2-1) & q-1 \\ 1 & -q & q-1 \\ 1 & 0 & -1 \end{pmatrix}.$$

因为 $P\neq Q$, 所以 $\widetilde{\text{Qua}}(2,\ q)$ 不自对偶.

表 8.17 Quad(2, q) 的特征值

	$C_0^{(2)}$	$C_{1,2}^{(2)}$
$f_0^{(2)}$	1	q^3-1
$f_1^{(2)},\ f_2^{(2)},\ f_{2^*}^{(2)}$	1	-1

2. $n=3$.

表 8.18 Qua(3, q) 的特征值

	$C_0^{(3)}$	$C_1^{(3)}$	$C_{2+}^{(3)}$	$C_{2-}^{(3)}$	$C_3^{(3)}$
$f_0^{(3)}$	1	q^3-1	$\frac{1}{2}q(q+1)(q^3-1)$	$\frac{1}{2}q(q-1)(q^3-1)$	$q^2(q-1)(q^3-1)$
$f_1^{(3)}$	1	-1	$\frac{1}{2}q(q+1)(q^2-1)$	$-\frac{1}{2}q(q-1)(q^2+1)$	$-q^2(q-1)$
$f_2^{(3)}$	1	-1	$\frac{1}{2}q(q^2-q-1)$	$\frac{1}{2}q(q^2-q+1)$	$-q^2(q-1)$
$f_{2^*}^{(3)}$	1	q^3-1	$-\frac{1}{2}q(q+1)$	$-\frac{1}{2}q(q-1)$	$-q^2(q-1)$
$f_3^{(3)}$	1	-1	$-\frac{1}{2}q(q+1)$	$-\frac{1}{2}q(q-1)$	q^2

表 8.19　$\widetilde{\mathrm{Q}}\mathrm{ua}(3, q)$ 的特征值

	$C_0^{(3)}$	$C_1^{(3)}$	$C_2^{(3)}$	$C_3^{(3)}$
$f_0^{(3)}$	1	q^3-1	$q^2(q^3-1)$	$q^2(q-1)(q^3-1)$
$f_1^{(3)}, f_2^{(3)}$	1	-1	$q^2(q-1)$	$-q^2(q-1)$
$f_{2^*}^{(3)}$	1	q^3-1	$-q^2$	$-q^2(q-1)$
$f_3^{(3)}$	1	-1	$-q^2$	q^2

表 8.20　Quad(3, q) 的特征值

	$C_0^{(3)}$	$C_{1,2}^{(3)}$	$C_3^{(3)}$
$f_0^{(3)}$	1	$(q^2+1)(q^3-1)$	$q^2(q-1)(q^3-1)$
$f_1^{(3)}, f_2^{(3)}, f_{2^*}^{(3)}$	1	$q^2(q-1)-1$	$-q^2(q-1)$
$f_3^{(3)}$	1	$-(q^2+1)$	q^2

第一特征值矩阵

$$P=\begin{pmatrix} 1 & (q^2+1)(q^3-1) & q^2(q-1)(q^3-1) \\ 1 & q^2(q-1)-1 & -q^2(q-1) \\ 1 & -(q^2+1) & q^2 \end{pmatrix}.$$

第二特征值矩阵

$$Q=q^6P^{-1}=\begin{pmatrix} 1 & (q^2+1)(q^3-1) & q^2(q-1)(q^3-1) \\ 1 & q^2(q-1)-1 & -q^2(q-1) \\ 1 & -(q^2+1) & q^2 \end{pmatrix}.$$

因为 $Q=P$, 所以 Quad(3, q) 自对偶.

3. $n=4$.

表 8.21　Qua(4, q) 的特征值

	$C_0^{(4)}$	$C_1^{(4)}$	$C_{2+}^{(4)}$	$C_{2-}^{(4)}$
$f_0^{(4)}$	1	q^4-1	$\frac{1}{2}q(q+1)(q^2+1)(q^3-1)$	$\frac{1}{2}q(q-1)(q^2+1)(q^3-1)$
$f_1^{(4)}$	1	-1	$\frac{1}{2}q(q^2+q+1)(q^3-1)$	$-\frac{1}{2}q(q-1)(q^4+q^2+1)$
$f_2^{(4)}$	1	-1	$\frac{1}{2}q(q^4+q^3-q^2-q-1)$	$\frac{1}{2}q(q^4-q^3+q^2-q+1)$
$f_{2^*}^{(4)}$	1	q^4-1	$\frac{1}{2}q(q+1)(q^3-q^2-1)$	$\frac{1}{2}q(q-1)(q^3-q^2-1)$
$f_3^{(4)}$	1	-1	$\frac{1}{2}q(q^3-q^2-q-1)$	$-\frac{1}{2}q(q-1)(q^2+1)$
$f_4^{(4)}$	1	-1	$-\frac{1}{2}q(q^2+q+1)$	$\frac{1}{2}q(q^2-q+1)$
$f_{4^*}^{(4)}$	1	q^4-1	$-\frac{1}{2}q(q+1)(q^2+1)$	$-\frac{1}{2}q(q-1)(q^2+1)$

续表

	$C_3^{(4)}$	$C_{4+}^{(4)}$	$C_{4-}^{(4)}$
$f_0^{(4)}$	$q^2(q^3-1)(q^4-1)$	$\frac{1}{2}\ q^4(q-1)(q^2+1)\cdot(q^3-1)$	$\frac{1}{2}\ q^4(q-1)(q^2-1)\cdot(q^3-1)$
$f_1^{(4)}$	$-q^2(q^3-1)$	$\frac{1}{2}q^4(q-1)(q^3-1)$	$-\frac{1}{2}q^4(q-1)(q^3-1)$
$f_2^{(4)}$	$-q^2(q^3-1)$	$-\frac{1}{2}q^4(q-1)$	$\frac{1}{2}q^4(q-1)$
$f_{2^*}^{(4)}$	$q^2(q^2-1)(q^3-q^2-1)$	$-\frac{1}{2}q^4(q-1)(q^2+1)$	$-\frac{1}{2}q^4(q-1)(q^2-1)$
$f_3^{(4)}$	q^2	$-\frac{1}{2}q^4(q-1)$	$\frac{1}{2}q^4(q-1)$
$f_4^{(4)}$	q^2	$\frac{1}{2}q^4$	$-\frac{1}{2}q^4$
$f_{4^*}^{(4)}$	$-q^2(q^4-1)$	$\frac{1}{2}q^4(q^2+1)$	$\frac{1}{2}q^4(q^2-1)$

表 8.22　$\widetilde{\mathrm{Q}}\mathrm{ua}(4,\ q)$ 的特征值

	$C_0^{(4)}$	$C_1^{(4)}$	$C_2^{(4)}=C_{2+}^{(4)}\cup C_{2-}^{(4)}$	$C_3^{(4)}$	$C_4^{(4)}=C_{4+}^{(4)}\cup C_{4-}^{(4)}$
$f_0^{(4)}$	1	q^4-1	$q^2(q^2+1)(q^3-1)$	$q^2\,(q^3-1)\cdot(q^4-1)$	$q^6(q-1)(q^3-1)$
$f_1^{(4)},\ f_2^{(4)}$	1	-1	$q^2(q^3-1)$	$-q^2(q^3-1)$	0
$f_{2^*}^{(4)}$	1	q^4-1	$q^2(q^3-q^2-1)$	$q^2\,(q^2-1)\cdot(q^3-q^2-1)$	$-q^6(q-1)$
$f_3^{(4)},\ f_4^{(4)}$	1	-1	$-q^2$	q^2	0
$f_{4^*}^{(4)}$	1	q^4-1	$-q^2(q^2+1)$	$-q^2(q^4-1)$	q^6

表 8.23　Quad(4, q) 的特征值

	$\sum_0=C_0^{(4)}$	$\sum_1=C_1^{(4)}\cup C_2^{(4)}$	$\sum_2=C_3^{(4)}\cup C_4^{(4)}$
$f_0^{(4)}$	1	$(q^2+1)(q^5-1)$	$q^2(q^3-1)(q^5-1)$
$f_1^{(4)},\ f_2^{(4)},\ f_{2^*}^{(4)}$	1	$q^2(q^3-1)-1$	$-q^2(q^3-1)$
$f_3^{(4)},\ f_4^{(4)},\ f_{4^*}^{(4)}$	1	$-(q^2+1)$	q^2

设 $n=4$, Quad(4, q) 的第一特征值矩阵为

$$P=\begin{pmatrix} 1 & (q^2+1)(q^5-1) & q^2(q^3-1)(q^5-1) \\ 1 & q^2(q^3-1)-1 & -q^2(q^3-1) \\ 1 & -(q^2+1) & q^2 \end{pmatrix}.$$

第二特征值矩阵为

$$Q = q^{10}P^{-1} = \begin{pmatrix} 1 & (q^2+1)(q^5-1) & q^2(q^3-1)(q^5-1) \\ 1 & q^2(q^3-1)-1 & -q^2(q^3-1) \\ 1 & -(q^2+1) & q^2 \end{pmatrix}.$$

易见 $Q = P$, 所以 Quad$(4, q)$ 是自对偶的.

参 考 文 献

1 Artin E. Geometric Algebra. New York-London: Interscience. 1957

2 Bannai E., Ito T. Algebraic Combinatorics I. Benjamin/Cummings Publishing Company. 1984

3 Brouwer A.E., Cohen A.M. , Neumajer A. Distance-Regular Graphs. Berlin Heidelberg: Springer-Verlag.1989

4 Egawa Y. Assocition Schemes of Quadratic forms. J.Combi-natorial Theory (A), 38. 1985. 1–14

5 华罗庚, 万哲先. 典型群. 上海: 上海科技出版社. 1993

6 霍元极, 祝学理. 利用对称矩阵构作多个结合类的结合方案. 应用数学学报, 10:3. 1987. 257–266

7 Huo Yuanji, Wan Zhexian. Non-symmetric Association Schemes of Symmetric Matrices. Chinese Science Bulletin, 36:18.1991. 1501–1505

8 Li Fenggao, Wang Yangxian. Subconstituents of dual polar graph in finite classical space III, Linear. Algebra and its Applications, 349.2002. 105–123

9 Ma Changli, Wang Yangxian. Automorphisms of Association Schemes of Quadratic Forms over a Finite Field of Characteristic Two. Algebra Colloguium, 10:1. 2003. 63–74

10 Ma Jianmin , Wang Yangxian. Note on Association Schemes of Symmetric Matrices in Characteristic 2. 河北师院学报 2. 1997. 1–7

11 A. Munemasa. The Geometry of Orthogonal Groups over Finite Fields. Tokya: Sophia University. 1996

12 A.Munemasa, D.V.Pasechnik , S.V.Shpectorov. The automorphism group and the convex subgraphs of the quadratic forms graph in characteristic two. J.Algebraic Combinatorics, 2(4). 1993. 411–419

13 M.E.Muzichuk. The automorphism group of the Paley graph. Yaroslavl: in "Voprosy Teorii Grup i Gomologicheskoy Algebry". 1987. 64–69

14 Wan Zhexian. Notes on finite geometries and the construction of PBIB designs VI, Some association schemes and PBIB designs based on finite geometries. Acta Scientia Sinica, 14:12. 1965. 1872–1876

15 Wan Zhexian. Geometry of Classical Groups over Finite Fields. Lund, Sweden/Chartwell-Bratt, Bromley, U.K.: Studentlitteratur. 1993

16 Wan Zhexian. Geometry of Matrices. Singapore: World Scientific. 1996

17 王仰贤. 利用矩阵构作多个结合类的结合方案. 应用数学学报, 3:2.1980. 97–195

18 Wang Yangxian, Ma Jianmin. Association Schemes of Symmetric Matrices over a Finite Field of Characteristic Two. J.Statistical Planning and Inference, 51. 1996.351–371

19 Wang Yangxian, Wang Chunsen, Ma Changli. Association schemes of quadratic forms over a finite field of characteristic two. Chinese Science Bulletin, 43:23. 1998. 1965–1968

20 王仰贤, 李风高, 霍元极. 有限典型空间中对偶极图的次成分 I. 应用数学学报, 24:3. 2001. 433–440

21 Wang Yangxian, Li Fenggao , Huo Yuanji. Subconstituents of Dual Polar Graph in Finite Classical Space II, Southeast Asian Bulletin of Mathemalics, 24. 2000. 643–654

22 Wang Yangxian, Wang Chunsen, Ma Changli, Ma Jianmin. Association Schemes of Quadratic Forms and Symmetric Bilinear Forms. J.Algebraic Combinatorics, 17. 2003. 149–161

23 麻常利. 二次型图的自同构及其应用. 博士学位论文, 河北师范大学. 2006

24 Feng Rongquan, Wang Yangxian, Ma Changli, Ma Jianmin. Eigenvalues of association schemes of quadratic forms. Discrete Mathematics. 2006

名 词 索 引

二 画

四 画

五 画

六 画

七 画

八 画

九 画

《现代数学基础丛书》已出版书目

(按出版时间排序)

1 数理逻辑基础（上册） 1981.1 胡世华、陆钟万 著
2 紧黎曼曲面引论 1981.3 伍鸿熙、吕以辇、陈志华 著
3 组合论（上册） 1981.10 柯召、魏万迪 著
4 数理统计引论 1981.11 陈希孺 著
5 多元统计分析引论 1982.6 张尧庭、方开泰 著
6 概率论基础 1982.8 严士健、王隽骧、刘秀芳 著
7 数理逻辑基础（下册） 1982.8 胡世华、陆钟万 著
8 有限群构造（上册） 1982.11 张远达 著
9 有限群构造（下册） 1982.12 张远达 著
10 环与代数 1983.3 刘绍学 著
11 测度论基础 1983.9 朱成熹 著
12 分析概率论 1984.4 胡迪鹤 著
13 巴拿赫空间引论 1984.8 定光桂 著
14 微分方程定性理论 1985.5 张芷芬、丁同仁、黄文灶、董镇喜 著
15 傅里叶积分算子理论及其应用 1985.9 仇庆久等 编
16 辛几何引论 1986.3 J.柯歇尔、邹异明 著
17 概率论基础和随机过程 1986.6 王寿仁 著
18 算子代数 1986.6 李炳仁 著
19 线性偏微分算子引论（上册） 1986.8 齐民友 著
20 实用微分几何引论 1986.11 苏步青等 著
21 微分动力系统原理 1987.2 张筑生 著
22 线性代数群表示导论（上册） 1987.2 曹锡华等 著
23 模型论基础 1987.8 王世强 著
24 递归论 1987.11 莫绍揆 著
25 有限群导引(上册) 1987.12 徐明曜 著
26 组合论（下册） 1987.12 柯召、魏万迪 著
27 拟共形映射及其在黎曼曲面论中的应用 1988.1 李忠 著
28 代数体函数与常微分方程 1988.2 何育赞 著

29　同调代数　1988.2　周伯壎　著
30　近代调和分析方法及其应用　1988.6　韩永生　著
31　带有时滞的动力系统的稳定性　1989.10　秦元勋等　编著
32　代数拓扑与示性类　1989.11　马德森著　吴英青、段海鲍译
33　非线性发展方程　1989.12　李大潜、陈韵梅　著
34　反应扩散方程引论　1990.2　叶其孝等　著
35　仿微分算子引论　1990.2　陈恕行等　编
36　公理集合论导引　1991.1　张锦文　著
37　解析数论基础　1991.2　潘承洞等　著
38　拓扑群引论　1991.3　黎景辉、冯绪宁　著
39　二阶椭圆型方程与椭圆型方程组　1991.4　陈亚浙、吴兰成　著
40　黎曼曲面　1991.4　吕以辇、张学莲　著
41　线性偏微分算子引论（下册）　1992.1　齐民友　著
42　复变函数逼近论　1992.3　沈燮昌　著
43　Banach 代数　1992.11　李炳仁　著
44　随机点过程及其应用　1992.12　邓永录等　著
45　丢番图逼近引论　1993.4　朱尧辰等　著
46　线性微分方程的非线性扰动　1994.2　徐登洲、马如云　著
47　广义哈密顿系统理论及其应用　1994.12　李继彬、赵晓华、刘正荣　著
48　线性整数规划的数学基础　1995.2　马仲蕃　著
49　单复变函数论中的几个论题　1995.8　庄圻泰　著
50　复解析动力系统　1995.10　吕以辇　著
51　组合矩阵论　1996.3　柳柏濂　著
52　Banach 空间中的非线性逼近理论　1997.5　徐士英、李冲、杨文善　著
53　有限典型群子空间轨道生成的格　1997.6　万哲先、霍元极　著
54　实分析导论　1998.2　丁传松等　著
55　对称性分岔理论基础　1998.3　唐云　著
56　Gel'fond-Baker 方法在丢番图方程中的应用　1998.10　乐茂华　著
57　半群的 S-系理论　1999.2　刘仲奎　著
58　有限群导引(下册)　1999.5　徐明曜等　著
59　随机模型的密度演化方法　1999.6　史定华　著
60　非线性偏微分复方程　1999.6　闻国椿　著
61　复合算子理论　1999.8　徐宪民　著
62　离散鞅及其应用　1999.9　史及民　编著

63 调和分析及其在偏微分方程中的应用 1999.10 苗长兴 著
64 惯性流形与近似惯性流形 2000.1 戴正德、郭柏灵 著
65 数学规划导论 2000.6 徐增堃 著
66 拓扑空间中的反例 2000.6 汪林、杨富春 编著
67 拓扑空间论 2000.7 高国士 著
68 非经典数理逻辑与近似推理 2000.9 王国俊 著
69 序半群引论 2001.1 谢祥云 著
70 动力系统的定性与分支理论 2001.2 罗定军、张祥、董梅芳 编著
71 随机分析学基础（第二版） 2001.3 黄志远 著
72 非线性动力系统分析引论 2001.9 盛昭瀚、马军海 著
73 高斯过程的样本轨道性质 2001.11 林正炎、陆传荣、张立新 著
74 数组合地图论 2001.11 刘彦佩 著
75 光滑映射的奇点理论 2002.1 李养成 著
76 动力系统的周期解与分支理论 2002.4 韩茂安 著
77 神经动力学模型方法和应用 2002.4 阮炯、顾凡及、蔡志杰 编著
78 同调论——代数拓扑之一 2002.7 沈信耀 著
79 金兹堡-朗道方程 2002.8 郭柏灵等 著
80 排队论基础 2002.10 孙荣恒、李建平 著
81 算子代数上线性映射引论 2002.12 侯晋川、崔建莲 著
82 微分方法中的变分方法 2003.2 陆文端 著
83 周期小波及其应用 2003.3 彭思龙、李登峰、谌秋辉 著
84 集值分析 2003.8 李雷、吴从炘 著
85 数理逻辑引论与归结原理 2003.8 王国俊 著
86 强偏差定理与分析方法 2003.8 刘文 著
87 椭圆与抛物型方程引论 2003.9 伍卓群、尹景学、王春朋 著
88 有限典型群子空间轨道生成的格（第二版） 2003.10 万哲先、霍元极 著
89 调和分析及其在偏微分方程中的应用（第二版） 2004.3 苗长兴 著
90 稳定性和单纯性理论 2004.6 史念东 著
91 发展方程数值计算方法 2004.6 黄明游 编著
92 传染病动力学的数学建模与研究 2004.8 马知恩、周义仓、王稳地、靳 祯 著
93 模李超代数 2004.9 张永正、刘文德 著
94 巴拿赫空间中算子广义逆理论及其应用 2005.1 王玉文 著
95 巴拿赫空间结构和算子理想 2005.3 钟怀杰 著
96 脉冲微分系统引论 2005.3 傅希林、闫宝强、刘衍胜 著

97　代数学中的Frobenius结构　2005.7　汪明义　著
98　生存数据统计分析　2005.12　王启华　著
99　数理逻辑引论与归结原理(第二版)　2006.3　王国俊　著
100　数据包络分析　2006.3　魏权龄　著
101　代数群引论　2006.9　黎景辉　陈志杰　赵春来　著
102　矩阵结合方案　2006.9　王仰贤　霍元极　麻常利　著